Hopf-Galois extensions and non-commutative rings

Fabio Alejandro Calderón Mateus

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C., Colombia
Abril de 2019

Hopf-Galois extensions and non-commutative rings

Fabio Alejandro Calderón Mateus
Mathematician

Thesis Work to Obtain the Degree of
Master in Science-Mathematics

Advisor
Armando Reyes, Ph.D.

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C., Colombia
Abril de 2019

TITLE

HOPF-GALOIS EXTENSIONS AND NON-COMMUTATIVE RINGS

TÍTULO

EXTENSIONES HOPF-GALOIS Y ANILLOS NO-CONMUTATIVOS

ABSTRACT: In this document we review the notion of Hopf Galois extensions, addressing remarkable examples, some properties and recent advances in such theory. Similarly, we present some families of non-commutative rings and algebras which arise in several applications and contexts. With particular examples, and using recent results on Hopf Galois theory, we study some interactions between such extensions and the mentioned families.

RESUMEN: En este documento abordaremos la noción de extensión Hopf Galois, revisando los ejemplos más destacados, algunas propiedades y los avances recientes en dicha teoría. De igual manera, presentamos algunas familias de anillos y álgebras no-conmutativas que aparecen en diversas aplicaciones y escenarios. Con ejemplos particulares, y usando trabajos recientes en teoría Hopf Galois, estudiamos algunas interacciones entre dichas extensiones y algunas de las familias mencionadas.

KEYWORDS: *Hopf Galois extension, quantum torsor, Hopf Galois system, Ore extension, almost symmetric algebra.*

PALABRAS CLAVE: *Extensión Hopf Galois, torsor cuántico, sistema Hopf Galois, extensión de Ore, algebra casi-simétrica.*

Dedicatory

To my mother, Gladys, for raising me to be the best person I could ever be.

To all my friends, for their support and encouragement.

To my professors, Lezama and Reyes, for teaching me the path of a good mathematician.

To my pets, Laika and Luna, for every night and morning brightened by their company.

To patience and perseverance, for they shall be the motto of every goal.

Acknowledgments

The academy is a path that one has to wander by itself, but not in solitude. I am grateful to so many people in such different ways that the list may never end. However, I will try my best to not left anyone out. My greatest gratitude goes to my Mother for everything through the years. Her unconditional love and support made possible every step in my journey so far.

No words are enough to thank Professor Armando Reyes, for his encouragement, support, and advice during the past four years. His young yet brilliant mind is a source of inspiration and respect. I also wish to express my heartfelt thanks to Professor Oswaldo Lezama, for being an example of a world-class mathematician and, more important, an excellent and humble human being.

I must thank my friends for every laugh in no matter what condition. Their commentaries and jokes, our afternoons of food and beer, and each cycling trip and day of study. Their friendship made my time at the National University of Colombia the best so far in my life.

Last, but not least, I am grateful to all the people at the National University of Colombia for their help during all these years. It is the place where I have met the most remarkable people, not only in the academic aspect but also in the human one. In particular, I am grateful to the Academic Direction and the Faculty of Sciences for their financial support.

CONTENTS

INTRODUCTION

> Discovery is a child's privilege. I mean the small child, the child who is not afraid to be wrong, to look silly, to not be serious, and to act differently from everyone else. He is also not afraid that the things he is interested in are in bad taste or turn out to be different from his expectations, from what they should be, or rather he is not afraid of what they actually are. He ignores the silent and flawless consensus that is part of the air we breathe – the consensus of all the people who are, or are reputed to be, reasonable.
>
> Alexander Grothendieck, *Crops and Seeds*

In the last half-century, Hopf algebras turned out to be a great tool for studying a large number of problems in several contexts: from providing solutions for the Yang-Baxter equation and describe the famous quantum groups –appearing in theoretical physics and algebraic theory–, to generalize Galois theory. And precisely, this last one instance is what concerns us in this document.

Classically, Galois theory studies and classifies automorphism groups of fields. In [CHR65] the theory was generalized to groups acting on commutative rings, and posteriorly, [CS69] extended those ideas, by replacing the action of a group on the algebra by the coaction of a Hopf algebra on a commutative algebra. The first general definition of Hopf Galois extensions is due to [KT81], although they restricted their study to the finite-dimensional case. In Chapter 1 we address the modern definition of such extensions, not without first recalling some basic notions regarding the theory of Hopf algebras. Our aim is to provide a large number of examples and properties, developing proofs and calculations that are usually omitted in the literature. We end the chapter giving two recent alternative approaches for Hopf Galois theory: quantum torsors, defined in [Gru03], and Hopf Galois systems, introduced by [Bic03a]. We address results relating these three notions.

Almost parallel to the first appearance of Hopf algebras, in [Ore33] a new class of non-commutative rings was defined, nowadays known as *skew polynomial rings* or *Ore extensions*. Although the aim of Ore was to find non-commutative algebras which could be embedded on division rings (cf. [Coh85]), these structures are per se a branch of study in algebra, as they allow us to describe many rings and algebras – most of them coming from physics mathematics and with wide applications in quantum mechanics. Therefore some classical results, such as Hilbert's Basis Theorem or Hilbert's Syzygy Theorem, have been generalized to these objects, while many other properties are still being studied. In [Cal16] we explored some interactions between Hopf

algebras and skew polynomial rings, based on the results of [Pan03] and [BOZZ15].

Thus, we star Chapter 2 reviewing basic definitions and results of skew polynomial rings, along with some remarkable examples. However, this is not the only family of non-commutative rings (or algebras) that has been defined since then. Inspired by the PBW theorem for enveloping algebras of Lie algebras, in [BG88] the so called *PBW extensions* were introduced. They consist of polynomial-type rings having a PBW basis and specific commutation rules. Moreover, [GL11] generalized such notion. Hence, our aim is to address these types of rings and the examples they comprehend. We close the chapter with a quite different collection of algebras, known as *almost symmetric algebras* or *Sridharan enveloping algebras*. They generalize enveloping algebras via twisting by 2-cocycles, without losing some nice properties.

With these two overviews, one could ask for the possible relations between some of these families and Hopf Galois extensions. Therefore, in Chapter 3 we review such interactions between skew polynomial rings and Hopf Galois extensions, studying the coactions of an arbitrary Hopf algebra over those objects. We also attach a Hopf Galois system to almost symmetric algebras and evidence the structure of quantum torsor present in Kashiwara algebras.

Notations and conventions. Throughout this document, all rings and morphisms are supposed to be unitary. K will denote an arbitrary commutative ring and $\Bbbk$ any field. Unless stated otherwise, tensor products are assumed to be over K and every K-module is supposed to be non-zero.

Let f, g, h be functions. If defined, we denote the composition of f with g by fg and the composition of h with itself n-times as h^n. $\mathrm{id}_X : X \to X$ will always denote the identity map of X.

Arrow diagrams will be constantly used; they represent composition of functions as concatenation of arrows. A diagram is said to be *commutative* if, no matter what path one follows, the composition of arrows (functions) gives always the same result.

The symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the usual numerical systems, assuming that $0 \in \mathbb{N}$.

CHAPTER 1

HOPF GALOIS EXTENSIONS: PRELIMINARIES, DEFINITIONS AND EXAMPLES

Although we assume some familiarity with the theory of Hopf algebras, for the purpose of a self-contained document, this chapter will start addressing some basic terminology of (co)algebras, bialgebras and Hopf algebras (Section 1.1), and their (co)modules and (co)actions (Section 1.2). Then we introduce in Section 1.3 the concept of Hopf Galois extension, which is transversal to this work; a large amount of examples and properties are presented. Finally, and following recent developments, we dedicate Sections 1.4 and 1.5 to two alternative (and equivalent) approaches to Hopf Galois extensions, namely quantum torsors and Hopf Galois systems.

1.1 HOPF ALGEBRAS

The starting point for the theory of Hopf algebras is restating the classical notion of an (unitary) algebra over a commutative ring in the language of arrows and commutative diagrams.

DEFINITION 1.1 (ALGEBRA, [MON93, DEFINITION 1.1.1]). A K-*algebra* is a K-module A together with two K-linear maps, $m : A \otimes A \to A$ and $u : K \to A$, such that the following diagrams are commutative:

$$\begin{array}{ccc} A\otimes A\otimes A & \xrightarrow{m\otimes \mathrm{id}_A} & A\otimes A \\ {\scriptstyle \mathrm{id}_A\otimes m}\downarrow & & \downarrow{\scriptstyle m} \\ A\otimes A & \xrightarrow[m]{} & A \end{array} \qquad \begin{array}{ccccc} & & A\otimes A & & \\ & {\scriptstyle u\otimes \mathrm{id}_A}\nearrow & \downarrow{\scriptstyle m} & \nwarrow{\scriptstyle \mathrm{id}_A\otimes u} & \\ K\otimes A & & & & A\otimes K \\ & \searrow^{\cong} & & \swarrow_{\cong} & \\ & & A & & \end{array} \tag{1.1}$$

(Associativity) (Unit property)

REMARK 1. Classically, a ring A is called a K-algebra if there exists a ring morphism $\phi : K \to A$ such that $\mathrm{Im}(\phi) \subseteq Z(A)$, where $Z(A)$ denotes the center of A. As expected, this formulation is equivalent to Definition 1.1 via the identification $ab = m(a \otimes b)$ and $u = \phi$. Thus the map

m is called the *multiplication* and u the *unity*. For this reason, we will assume familiarity with classical definitions for algebras (namely ideals, modules, bimodules, etc.). Moreover, for convenience, for any given algebra A, we will simply write $ab := m(a \otimes b)$ for the multiplication and $1_A := u(1_K)$ for its unit element.

The purpose of replacing standard definitions for this one is that of being able to reverse arrows and hence obtain the dual concept.

DEFINITION 1.2 (COALGEBRA, [MON93, DEFINITION 1.1.3]). A *K-coalgebra* is a K-module C together with two K-linear maps, $\Delta : C \to C \otimes C$ and $\varepsilon : C \to K$, such that the following diagrams are commutative:

$$\begin{array}{ccc} C & \xrightarrow{\Delta} & C \otimes C \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_C \otimes \Delta} \\ C \otimes C & \xrightarrow[\Delta \otimes \mathrm{id}_C]{} & C \otimes C \otimes C \end{array} \qquad \begin{array}{ccccc} & & C & & \\ & \swarrow^{\cong} & \downarrow{\scriptstyle\Delta} & \searrow^{\cong} & \\ K \otimes C & & & & C \otimes K \\ & {\scriptstyle\varepsilon \otimes \mathrm{id}_C}\nwarrow & & \nearrow{\scriptstyle \mathrm{id}_C \otimes \varepsilon} & \\ & & C \otimes C & & \end{array} \tag{1.2}$$

(Coassociativity) (Counit property)

The map Δ is called the *comultiplication* and ε the *counit*.

REMARK 2. Notice that the right diagram of (1.2) gives that Δ is injective, just as the right one from (1.1) means that m is surjective.

As one can expect, arrows between these structures are defined as those preserving the operations.

DEFINITION 1.3 (MORPHISM OF ALGEBRAS, [DNR01, DEFINITION 1.1.14]). Let A, B be two K-algebras. A K-linear map $f : A \to B$ is said to be an *algebra morphism*, if the following diagrams are commutative:

$$\begin{array}{ccc} A \otimes A & \xrightarrow{f \otimes f} & B \otimes B \\ {\scriptstyle m_A}\downarrow & & \downarrow{\scriptstyle m_B} \\ A & \xrightarrow[f]{} & B \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle u_A}\nwarrow \quad \nearrow{\scriptstyle u_B} & \\ & K & \end{array}$$

DEFINITION 1.4 (MORPHISM OF COALGEBRAS, [DNR01, DEFINITION 1.1.14]). Let C, D be two K-coalgebras. A K-linear map $g : C \to D$ is said to be an *coalgebra morphism*, if the following diagrams are commutative:

$$\begin{array}{ccc} C & \xrightarrow{g} & D \\ {\scriptstyle\Delta_C}\downarrow & & \downarrow{\scriptstyle \Delta_D} \\ C \otimes C & \xrightarrow[g \otimes g]{} & D \otimes D \end{array} \qquad \begin{array}{ccc} C & \xrightarrow{g} & D \\ & {\scriptstyle\varepsilon_C}\searrow \quad \swarrow{\scriptstyle \varepsilon_D} & \\ & K & \end{array}$$

By writing down some diagrams, one can easily verify that the composition of morphisms, in either case, is well defined. Therefore we can consider $K-\mathrm{Alg}$, the category of K-algebras, and $K-\mathrm{Cog}$, the category of K-coalgebras. Several properties of these two are studied in [DNR01, §1.4]; we only mention here the subobjects and factor objects of $K-\mathrm{Cog}$.

DEFINITION 1.5 (SUBCOALGEBRA, [DNR01, DEFINITION 1.4.1]). Let C be a K-coalgebra. A submodule D of C is called a *subcoalgebra of* C, if $\Delta(D) \subseteq D \otimes D$.

DEFINITION 1.6 (LEFT, RIGHT AND BILATERAL COIDEAL, [DNR01, DEFINITION 1.4.3]). Let C be a K-coalgebra and I a submodule of C.

(i) I is called a *left coideal of* C, if $\Delta(I) \subseteq C \otimes I$.

(ii) I is called a *right coideal of* C, if $\Delta(I) \subseteq I \otimes C$.

(iii) I is called a *coideal of* C, if $\Delta(I) \subseteq I \otimes C + C \otimes I$ and $\varepsilon(I) = 0$.

Despite the intuition provided by classical notions over algebras, one must be careful, since not necessarily the respective ones in coalgebra theory behave equally. For example, if I is a coideal, it does not follows that I is a left or right coideal (cf. [DNR01, Exercise 1.4.4]).

Given M, N two K-modules, the *twist map* $\tau_{M,N} : M \otimes N \to N \otimes M$ is defined by $m \otimes n \mapsto n \otimes m$, for all $m \in M$ and $n \in N$. This arrow is always a K-isomorphism (cf. [AM69, Proposition 2.14]), and sometimes is also denoted as $\tau_{(12)}$ when emphasis in the interchanged coordinates is needed. In the situation $M = N$, we simply write τ_M. The twist map allows us to define when an algebra is commutative, and hence, dualize the concept to coalgebras.

DEFINITION 1.7 (COMMUTATIVE ALGEBRA, [DNR01, DEFINITION 1.1.13]). A K-algebra A is said to be *commutative*, if the following diagram is commutative:

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\tau_A} & A \otimes A \\ & {\scriptstyle m} \searrow \quad \swarrow {\scriptstyle m} & \\ & A & \end{array}$$

DEFINITION 1.8 (COCOMMUTATIVE COALGEBRA, [DNR01, DEFINITION 1.1.13]). A K-coalgebra C is said to be *cocommutative*, if the following diagram is commutative:

$$\begin{array}{ccc} & C & \\ & {\scriptstyle \Delta} \swarrow \quad \searrow {\scriptstyle \Delta} & \\ C \otimes C & \xrightarrow[\tau_C]{} & C \otimes C \end{array}$$

NOTATION. If M is a K-module, for $n \geq 2$, we denote

$$M^{\otimes n} := \underbrace{M \otimes M \otimes \cdots \otimes M}_{n\text{-times}}.$$

By definition, $M^{\otimes 0} := K$ and $M^{\otimes 1} := M$. Furthermore, for any coalgebra C, we recurrently define the sequence of maps $\{\Delta_n : C \to C^{\otimes(n+1)}\}_{n\geq 1}$ as follows:

$$\Delta_1 := \Delta,$$
$$\Delta_n := \left(\Delta \otimes \mathrm{id}_C^{n-1}\right)\Delta_{n-1}, \qquad \text{for any } n \geq 2.$$

Notice that, whereas in an algebra A the multiplication is a straightforward application of a rule $m : A\otimes A \to A$, in a coalgebra C the comultiplication $\Delta : C \to C\otimes C$ will always give an element in the tensor module, whose elements are known for not being calculation-friendly. Hence, we adopt the notation introduced in [Swe69, §1.2], which will relieve proofs and calculations.

NOTATION (SWEEDLER'S SIGMA NOTATION, [MON93, §1.4]). Let C be a K-coalgebra. Given $c \in C$, the element $\Delta(c)$ of $C \otimes C$ has the form

$$\Delta(c) = \sum_{i=1}^{n} c_{i1} \otimes c_{i2}, \qquad \text{for some } c_{i1}, c_{i2} \in C.$$

For simplicity we will get ride of the subscripts and write the above as

$$\Delta(c) = \sum c_1 \otimes c_2 \qquad \text{or} \qquad \Delta(c) = \sum c_{(1)} \otimes c_{(2)}.$$

The second one shall be used mostly when several operations (other than comultiplication) are involved. As we will do in Section 1.5, sometimes even the summation symbol is suppressed.

This notation is handy in the sense that we can state some properties of the comultiplication in a simpler way. For example, the coassociativity of Δ (left of (1.2)) states that

$$\sum \left(\sum c_{11} \otimes c_{12}\right) \otimes c_2 = \sum c_1 \otimes \left(\sum c_{21} \otimes c_{22}\right),$$

and therefore we are able to just write

$$\Delta_2(c) = \sum c_1 \otimes c_2 \otimes c_3$$

Moreover, we will have

$$\Delta_n(c) = \sum c_1 \otimes \cdots \otimes c_{n+1}, \qquad \text{for any } n \geq 1.$$

We also may reformulate the main property of the counit (right of (1.2)) as

$$\sum \varepsilon(c_1)c_2 = c = \sum c_1 \varepsilon(c_2).$$

The behavior of a coalgebra morphism $g : C \to D$ can be state as

$$\sum g(c)_1 \otimes g(c)_2 = \sum g(c_1) \otimes g(c_2).$$

Now, suppose that H is an algebra over K in which we were able to define also a K-coalgebra structure. The obvious question is whether, in some way, the operations involved are related. In that sense, the next result provides some compatibility essential in the bialgebra structure.

LEMMA 1.1 ([DNR01, PROPOSITION 4.1.1]). *Let H be a K-module which is simultaneously endowed with an algebra and a coalgebra structure, both over K. Then the following assertions are equivalent:*

(i) *The maps m and u are morphisms of coalgebras.*

(ii) *The maps Δ and ε are morphisms of algebras.*

Proof. As we shall see later in Examples 1.1 and 1.2, $H \otimes H$ and K also acquire algebra and coalgebra structures over K via

$$\Delta_{H\otimes H} = \Delta_H \otimes \Delta_H, \qquad m_{H\otimes H} = m_H \otimes m_H, \qquad u_{H\otimes H} = (u_H \otimes u_H)\Delta_K,$$
$$\varepsilon_{H\otimes H} = m_K(\varepsilon_H \otimes \varepsilon_H), \qquad \Delta_K = \mathrm{id}_K \otimes 1, \qquad u_K = \varepsilon_K = \mathrm{id}_K .$$

Hence, by definition, m_H is a morphism of coalgebras if and only if the diagrams

$$\begin{array}{ccc} H\otimes H & \xrightarrow{m_H} & H \\ {\scriptstyle \Delta_{H\otimes H}}\downarrow & & \downarrow{\scriptstyle \Delta_H} \\ H\otimes H\otimes H\otimes H & \xrightarrow[m_H\otimes m_H]{} & H\otimes H \end{array} \qquad \begin{array}{ccc} H\otimes H & \xrightarrow{m_H} & H \\ & {\scriptstyle \varepsilon_{H\otimes H}}\searrow \quad \swarrow{\scriptstyle \varepsilon_H} & \\ & K & \end{array} \tag{1.3}$$

are commutative. Similarly, u_H is a morphism of coalgebras if and only if the diagrams

$$\begin{array}{ccc} K & \xrightarrow{u_H} & H \\ {\scriptstyle \Delta_K}\downarrow & & \downarrow{\scriptstyle \Delta_H} \\ K\otimes K & \xrightarrow[u_H\otimes u_H]{} & H\otimes H \end{array} \qquad \begin{array}{ccc} K & \xrightarrow{u_H} & H \\ & {\scriptstyle \varepsilon_K}\searrow \quad \swarrow{\scriptstyle \varepsilon_H} & \\ & K & \end{array} \tag{1.4}$$

are commutative. Notice that diagrams in (1.3) can be rewritten as

$$\begin{array}{ccc} H\otimes H & \xrightarrow{\Delta_H\otimes\Delta_H} & H\otimes H\otimes H\otimes H \\ {\scriptstyle m_H}\downarrow & & \downarrow{\scriptstyle m_{H\otimes H}} \\ H & \xrightarrow[\Delta_H]{} & H\otimes H \end{array} \qquad \begin{array}{ccc} H\otimes H & \xrightarrow{\varepsilon_H\otimes\varepsilon_H} & K\otimes K \\ {\scriptstyle m_H}\downarrow & & \downarrow{\scriptstyle m_K} \\ H & \xrightarrow[\varepsilon_H]{} & K \end{array} \tag{1.5}$$

and the ones in (1.4) as

$$\begin{array}{ccc} H & \xrightarrow{\Delta_H} & H\otimes H \\ & {\scriptstyle u_H}\searrow \quad \swarrow{\scriptstyle u_{H\otimes H}} & \\ & K & \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{\varepsilon_H} & K \\ & {\scriptstyle u_H}\searrow \quad \swarrow{\scriptstyle u_K} & \\ & K & \end{array} \tag{1.6}$$

Referring again to definitions, one can see that Δ_H is a morphism of algebras if and only if both left diagrams of (1.5) and (1.6) are commutative. Similarly, ε_H is a morphism of algebras if and

only if both right diagrams of (1.5) and (1.6) are commutative. Hence, by transitivity on the implications above, we have shown (i) $\Leftrightarrow$ (ii). □

This allows us to define the notion of bialgebra and arrows between them.

DEFINITION 1.9 (BIALGEBRA, [MON93, DEFINITION 1.3.1]). A *K-bialgebra* is a K-module H endowed simultaneously with both algebra and coalgebra structure over K in which m and u are morphisms of coalgebras.

REMARK 3. For simplicity, and since it holds for most applications, throughout we will require every K-bialgebra H to be flat over K, meaning that the tensor product functor $-\otimes H$ is exact (i.e., preserves the exactness of sequences).

DEFINITION 1.10 (BIALGEBRA MORPHISM, [MON93, DEFINITION 1.3.1]). Let H, L be two K-coalgebras. A K-linear map $f : H \to L$ is said to be an *bialgebra morphism*, if it is both algebra and coalgebra morphism.

The category of K-bialgebras is denoted by $K-$Bialg.

We are still laking one last operation involved in the constitution of a Hopf algebra. For that, we will give an algebra structure to the module of all K-linear maps between a coalgebra C and an algebra A, $\mathrm{Hom}_K(C,A)$. The *convolution product* is defined as

$$(f*g)(c) := \big(m_A(f\otimes g)\Delta_C\big)(c), \qquad \text{for all } f,g\in \mathrm{Hom}_K(C,A) \text{ and all } c\in C. \tag{1.7}$$

In Sweedler's sigma notation, this can be rewritten as

$$(f*g)(c) = \sum f(c_1)g(c_2).$$

PROPOSITION 1.2. *If C is a K-coalgebra and A is a K-algebra, then the convolution product over $\mathrm{Hom}_K(C,A)$ given by (1.7) is associative and the identity element is $u_A\varepsilon_C$. Hence $\mathrm{Hom}_K(C,A)$ is a K-algebra.*

Proof. Using Sweedler's sigma notation, for $g, f, h \in \mathrm{Hom}_K(C,A)$ and $c\in C$, we have

$$\big((f*g)*h\big)(c) = \sum (f*g)(c_1)h(c_2) = \sum f(c_1)g(c_2)h(c_3) = \sum f(c_1)(g*h)(c_2) = \big(f*(g*h)\big)(c).$$

On the other hand,

$$\big((u\varepsilon)*f\big)(c) = \sum (u\varepsilon)(c_1)f(c_2) = \sum \varepsilon(c_1)f(c_2) = f\Big(\sum \varepsilon(c_1)c_2\Big) = f(c),$$

and hence $(u\varepsilon)*f = f$. Similarly $f*(u\varepsilon) = f$. □

Notice that the coassociativity was used above, which in the eyes of Sweedler's sigma notation can be misunderstood as a sloppy manipulation of indexes; one shall not be deceived (cf. [DNR01, 1.1.11]).

Due to Proposition 1.2, we say that $f\in \mathrm{Hom}_K(C,A)$ is *convolution invertible* if f is invertible in $\mathrm{Hom}_K(C,A)$, that is, if there exists $g\in \mathrm{Hom}_K(C,A)$ such that $f*g = g*f = u_A\varepsilon_C$.

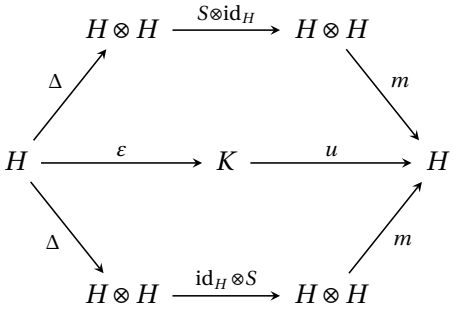
Now, in the particular case of H being a K-bialgebra, we can consider the convolution product on $\mathrm{Hom}_K(H,H)$, understanding the first appearance of H as coalgebra and the second as algebra. Notice that $\mathrm{id}_H \in \mathrm{Hom}_K(H,H)$; however, not necessarily it is convolution invertible (cf. [DNR01, Example 4.3.1]). In the affirmative case, H is called a Hopf algebra.

DEFINITION 1.11 (HOPF ALGEBRA, [MON93, DEFINITION 1.5.1]). Let H be a K-bialgebra. H is said to be a *K-Hopf algebra*, if there exists an element $S \in \mathrm{Hom}_K(H,H)$ which is an inverse to id_H under the convolution product. In this case, S is called an *antipode* for H.

REMARK 4. Since $\mathrm{Hom}_K(H,H)$ is an algebra and the antipode S is defined as an inverse, it is unique. Moreover, using Sweedler's sigma notation, S satisfies

$$\sum S(h_1)h_2 = \varepsilon(h)1 = \sum h_1 S(h_2), \qquad \text{for all } h \in H, \tag{1.8}$$

which can be restated as the commutativity of the following diagram:



Similarly to previous structures, arrows can be considered between Hopf algebras and therefore one can define the corresponding category, denoted by $K-$HopfAlg.

DEFINITION 1.12 (MORPHISM OF HOPF ALGEBRAS, [DNR01, DEFINITION 4.2.4]). Let H, L be two K-Hopf algebras. A morphism of K-bialgebras $f : H \to L$ is said to be a *Hopf algebra morphism*, if $f S_H(h) = S_L f(h)$ for all $h \in H$.

REMARK 5. In fact, it can be shown that any bialgebra morphism between two Hopf algebras is always a Hopf algebra morphism (cf. [DNR01, Proposition 4.2.5]). In terms of categories, it means that $K-$HopfAlg is a full subcategory of $K-$Bialg.

The subobjects and the factor objects of $K-$HopfAlg are defined as follows.

DEFINITION 1.13 (HOPF SUBALGEBRA, [DNR01, DEFINITION 4.2.12]). Let H be a Hopf algebra. A K-submodule A of H is called a *Hopf subalgebra*, if it is a subalgebra of H, a subcoalgebra of H and $S(A) \subseteq A$.

DEFINITION 1.14 (HOPF IDEAL, [MON93, DEFINITION 1.5.1]). Let H be a Hopf algebra. A K-submodule I of H is called a *Hopf ideal*, if it is an ideal of H (as algebra), a coideal of H (as coalgebra) and $S(I) \subseteq I$.

Before some examples, we give additional notions and results related to Hopf algebras that will be used throughout this document.

PROPOSITION 1.3 ([DNR01, PROPOSITION 4.2.6]). *Let H be a Hopf algebra. Then, for any*

$g, h \in H$, the following assertions hold:

(i) $S(hg) = S(g)S(h)$.

(ii) $S(1) = 1$.

(iii) $\Delta(S(h)) = \sum S(h_2) \otimes S(h_1)$.

(iv) $\varepsilon(S(h)) = \varepsilon(h)$.

Properties (i)-(ii) mean that S is an *anti-morphism of algebras*, while (iii)-(iv) that S is an *anti-morphism of coalgebras*.

In any coalgebra, elements whose comultiplication has a remarkable form are very important. We name them.

DEFINITION 1.15 (GROUP-LIKE AND PRIMITIVE ELEMENTS, [DNR01, DEFINITION 1.4.13]). Let C be a coalgebra. For an element $c \in C$, we say that:

(i) c is a *group-like element*, if $\Delta(c) = c \otimes c$. $G(C)$ denotes the set of all group-like elements.

(ii) c is a *primitive element*, if $\Delta(c) = c \otimes 1 + 1 \otimes c$. $P(C)$ denotes the set of all primitive elements.

(iii) c is a *g-h-primitive element*, or simply a *skew primitive element* when g and h are not specified, if $\Delta(c) = c \otimes g + h \otimes c$. $P_{g,h}(C)$ denotes the set of all g-h-primitive elements.

In particular, if H is a Hopf algebra, group-like elements acquire an important role.

PROPOSITION 1.4 ([DNR01, REMARK 4.2.9]). *Let H be a Hopf algebra. Then $G(H)$ is a group with induced multiplication.*

Proof. Since Δ is an algebra morphism, for any $f, g \in G(H)$ we have

$$\Delta(fg) = \Delta(f)\Delta(g) = (f \otimes f)(g \otimes g) = fg \otimes fg$$

and hence $fg \in G(H)$. The same argument shows that $1 \in G(H)$. Finally, if $g \in G(H)$, then $S(g)$ is also a group-like element (cf. Proposition 1.3). Hence, $g^{-1} = S(g)$. Indeed, by relation (1.8) and using that $\Delta(g) = g \otimes g$, we get $S(g)g = \varepsilon(g)1 = u\varepsilon(g)$. □

We end this section with some examples. For a larger amount refer to [DNR01], [Kas95], [Mon93] or [Swe69], since only a few, widely used in this document, shall be mentioned.

EXAMPLE 1.1 (COMMUTATIVE RINGS AND FIELDS). Any commutative ring K has structure of K-Hopf algebra by putting, for all $k, k' \in K$,

$$m : K \otimes K \to K, \quad m(k \otimes k') := kk'; \qquad u : K \to K, \quad u(k) := k;$$
$$\Delta : K \to K \otimes K, \quad \Delta(k) := k \otimes 1; \qquad \varepsilon : K \to K, \quad \varepsilon(k) := k;$$
$$S : S \to S, \quad S(k) := k,$$

Indeed, since the map $K\times K\to K$ given by $(k,k')\mapsto kk'$ is bilinear, m is a K-linear map; obviously $u=\mathrm{id}_K$, which is also a K-linear map. Moreover,

$$\begin{aligned}[m(m\otimes \mathrm{id}_K)](k\otimes k'\otimes k'') &= m(kk'\otimes k'') = (kk')k'' = k(k'k'') = m(k\otimes k'k'')\\ &= [m(\mathrm{id}_K\otimes m)](k\otimes k'\otimes k''),\\ [m(\mathrm{id}_K\otimes u)](k\otimes k') &= m(k\otimes u(k')) = m(k\otimes k') = kk',\\ [m(u\otimes \mathrm{id}_K)](k\otimes k') &= m(u(k)\otimes k') = m(k\otimes k') = kk',\end{aligned}$$

which proves the commutativity of the diagrams in (1.1); hence K is a K-algebra. Similarly, since Δ and ε are K-linear and

$$\begin{aligned}[(id_K\otimes\Delta)\Delta](k) &= (\mathrm{id}_K\otimes\Delta)(k\otimes 1) = k\otimes 1\otimes 1 = (\Delta\otimes\mathrm{id}_K)(k\otimes 1) = [(\Delta\otimes\mathrm{id}_K)\Delta](k),\\ [(\varepsilon\otimes\mathrm{id}_K)\Delta](k) &= (\varepsilon\otimes\mathrm{id}_K)(k\otimes 1) = \varepsilon(k)\otimes 1 = k\otimes 1,\\ [(\mathrm{id}_K\otimes\varepsilon)\Delta](k) &= (\mathrm{id}_K\otimes\varepsilon)(k\otimes 1) = k\otimes\varepsilon(1) = k\otimes 1,\end{aligned}$$

the commutativity of (1.2) is shown and thus K is a K-coalgebra. The verification of Δ and ε being morphisms of K-algebras is straightforward, although it uses that $K\otimes K$ is an algebra (cf. Example 1.2 below). Finally, since

$$\begin{aligned}[m(S\otimes\mathrm{id}_K)\Delta](k) &= [m(S\otimes\mathrm{id}_K)](k\otimes 1) = m(S(k)\otimes 1) = m(k\otimes 1) = k = u\varepsilon(k),\\ [m(\mathrm{id}_K\otimes S)\Delta](k) &= [m(\mathrm{id}_K\otimes S)](k\otimes 1) = m(k\otimes S(1)) = m(k\otimes 1) = k = u\varepsilon(k),\end{aligned}$$

S is an antipode for H and hence K is a K-Hopf algebra. In particular, this holds if $K=\Bbbk$ is a field.

The next example establish a methodical way of constructing new Hopf algebras.

EXAMPLE 1.2 (TENSOR PRODUCT). Let A,B be two K-algebras. Then the K-module $A\otimes B$ has also structure of K-algebra with multiplication $m_{A\otimes B}$ and unit $u_{A\otimes B}$ given by the compositions

$$\begin{aligned}m_{A\otimes B}\colon\ (A\otimes B)\otimes(A\otimes B) &\xrightarrow{\mathrm{id}_A\otimes\tau_{A,B}\otimes\mathrm{id}_B} (A\otimes A)\otimes(B\otimes B) \xrightarrow{m_A\otimes m_B} A\otimes B,\\ u_{A\otimes B}\colon\ K &\xrightarrow{\cong} K\otimes K \xrightarrow{u_A\otimes u_B} A\otimes B.\end{aligned}$$

Notice that the multiplication can be stated as

$$(a\otimes b)(a'\otimes b') := aa'\otimes bb',\quad \text{for all } a,a'\in A,\ b,b'\in B.$$

The unit element is $1_A\otimes 1_B$. Further results on this algebra can be found in [Kas95, §II.4]. When $A=B$ the multiplication simplifies to $m_{A\otimes A}:=m_A\otimes m_A$.

Similarly, if C,D are two K-coalgebras, then $C\otimes D$ has also structure of K-coalgebra with comultiplication $\Delta_{C\otimes D}$ given by the composition

$$\Delta_{C\otimes D}\colon\ C\otimes D \xrightarrow{\Delta_C\otimes\Delta_D} (C\otimes C)\otimes(D\otimes D) \xrightarrow{\mathrm{id}_C\otimes\tau_{C,D}\otimes\mathrm{id}_D} (C\otimes D)\otimes(C\otimes C)$$

and counit $\varepsilon_{C\otimes D}$ defined as

$$\varepsilon_{C\otimes D}\colon\ C\otimes D \xrightarrow{\varepsilon_C\otimes\varepsilon_D} K\otimes K \xrightarrow{\cong} K.$$

In Sweedler's sigma notation,

$$\Delta_{C\otimes D}(c\otimes d)=\sum(c\otimes d)_1\otimes(c\otimes d)_2=\sum(c_1\otimes d_1)\otimes(c_2\otimes d_2),$$
$$\varepsilon_{C\otimes D}(c\otimes d)=\varepsilon_C(c)\varepsilon_D(d).$$

When $C=D$ the comultiplication simplifies to $\Delta_{C\otimes C}:=\Delta_C\otimes\Delta_C$.

Furthermore, if H,L are two K-Hopf algebras, then their tensor product is also a K-Hopf algebra with antipode $S_{H\otimes L}:=S_H\otimes S_L$.

Recall that for any $\Bbbk$-vector space V, we denote by $V^*:=\mathrm{Hom}_\Bbbk(V,\Bbbk)$ its *dual vector space* (also called the *linear dual* of V), consisting of all $\Bbbk$-linear maps from V to $\Bbbk$ together with the pointwise addition and scalar multiplication by constants. In particular, we have $\Bbbk^*\cong\Bbbk$ via the identification $f\mapsto f(1_\Bbbk)$ (cf. [Hun74, Theorem IV.4.9]). This allow us to introduce the next example.

EXAMPLE 1.3 (LINEAR DUAL OF A FINITE DIMENSIONAL HOPF ALGEBRA). Let H be a $\Bbbk$-Hopf algebra such that H is finite dimensional as $\Bbbk$-vector space. Then its linear dual H^* is also a $\Bbbk$-Hopf algebra with multiplication and unity

$$m^\circ\colon\ H^*\otimes H^* \xrightarrow{\cong} (H\otimes H)^* \xrightarrow{\Delta^*} H^*,$$
$$u^\circ\colon\ \Bbbk \xrightarrow{\cong} \Bbbk^* \xrightarrow{\varepsilon^*} H^*,$$

comultiplication and counity

$$\Delta^\circ\colon\ H^* \xrightarrow{m^*} (H\otimes H)^* \xrightarrow{\cong} H^*\otimes H^*,$$
$$\varepsilon^\circ\colon\ H^* \xrightarrow{u^*} \Bbbk^* \xrightarrow{\cong} \Bbbk,$$

and antipode

$$S^\circ\colon\ H^* \xrightarrow{S^*} H^*.$$

REMARK 6. In Example 1.3 the condition of H being finite dimensional can not be easily dropped, for if H is not finite dimensional, $H^*\otimes H^*$ could be a proper subspace of $(H\otimes H)^*$ and thus the image of $m^\circ: H^*\to(H\otimes H)^*$ may not lie in $H^*\otimes H^*$. Therefore, for the general case, a certain subset H° of H^* is considered, often called the *finite dual* of H (cf. [Mon93, Chapter 9] or [DNR01, §1.5]).

On the other hand, dual Hopf algebras for those defined over commutative rings constitute an open line of investigation, and some progress has been made when the base ring is a polynomial algebra (cf. [Kur02]).

EXAMPLE 1.4 (QUOTIENT OF A HOPF ALGEBRA). Let H be a K-Hopf algebra and I a Hopf ideal of H. Since I is a two-sided ideal of H, the quotient module H/I already has structure of K-algebra,

by putting

$$\overline{h}\overline{g} := \overline{hg}, \qquad \text{for all } h, g \in H,$$

where $\overline{h} := h + I$. Notice that the identity element is $\overline{1}$. Moreover, H/I has Hopf algebra structure given by

$$\overline{\Delta}(\overline{h}) := \sum \overline{h_1} \otimes \overline{h_2}, \qquad \overline{\varepsilon}(\overline{h}) := \varepsilon(h) \qquad \text{and} \qquad \overline{S}(\overline{h}) := \overline{S(h)}, \qquad \text{for all } h \in H.$$

One can easily check that the canonical projection $H \to H/I$ is a surjective morphism of Hopf algebras.

In the following examples, the base ring is a field.

EXAMPLE 1.5 (GROUP ALGEBRA). Let G be a (multiplicative) group. The *group algebra*, denoted by $\Bbbk G$, is the $\Bbbk$-vector space with basis $\{g \in G\}$, and hence its elements are of the form

$$\sum_{g \in G} k_g g,$$

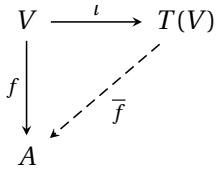
where only finite k_g are non-zero elements of $\Bbbk$. $\Bbbk G$ is a $\Bbbk$-algebra with multiplication given by (cf. [Hun74, p. 117])

$$\left(\sum_{i=1}^{n} k_i g_i\right)\left(\sum_{j=1}^{m} l_j h_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} (k_i l_j)(g_i h_j), \qquad \text{for all } k_i, l_j \in \Bbbk,\ g_i, h_j \in G.$$

Furthermore, $\Bbbk G$ becomes a $\Bbbk$-Hopf algebra by linearly extending the following rules:

$$\Delta(g) := g \otimes g, \qquad \varepsilon(g) := 1 \qquad \text{and} \qquad S(g) := g^{-1}, \qquad \text{for all } g \in G.$$

EXAMPLE 1.6 (TENSOR ALGEBRA). Let V be a $\Bbbk$-vector space. A $\Bbbk$-algebra $T(V)$ is said to be a *tensor algebra of* V, if there exists a $\Bbbk$-linear map $\iota : V \to T(V)$ such that the following universal property is satisfied: *for any $\Bbbk$-algebra A and any $\Bbbk$-linear map $f : V \to A$ there exists an unique algebra morphism $\overline{f} : T(V) \to A$ such that the following diagram is commutative:*



It can be shown that $T(V)$ is unique up to isomorphism (cf. [Lez19b, §3.5]) and that it can be described as

$$T(V) := \bigoplus_{i \geq 0} V^{\otimes i},$$

meaning that any element of $T(V)$ has the form $z = (z_i)_{i \geq 0}$, where $z_i \in V^{\otimes n}$ and almost all z_i vanish. The multiplication is given by the rule

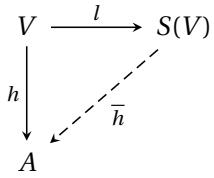
$$(v_1 \otimes \cdots \otimes v_i)(v_{i+1} \otimes \cdots \otimes \otimes v_{i+j}) = v_1 \otimes \cdots \otimes v_{i+j}, \qquad \text{for all } i, j \geq 0.$$

Notice that the identity element is $1 \in V^{\otimes 0} = \Bbbk$. $T(V)$ becomes a $\Bbbk$-Hopf algebra by extending (via the universal property) the rules

$$\Delta(v) := v \otimes 1 + 1 \otimes v, \qquad \varepsilon(v) := 0 \qquad \text{and} \qquad S(v) := -v, \qquad \text{for all } v \in V. \tag{1.9}$$

A complete proof of this can be found in [DNR01, 4.3.2].

EXAMPLE 1.7 (SYMMETRIC ALGEBRA). Let V be a $\Bbbk$-vector space. A commutative $\Bbbk$-algebra $S(V)$ is said to be a *symmetric algebra of* V, if there exists a $\Bbbk$-linear map $l : V \to S(V)$ such that the following universal property is satisfied: *for any commutative $\Bbbk$-algebra A, if $h : V \to A$ is a $\Bbbk$-linear map, then there exists an unique algebra morphism $\overline{h} : S(V) \to A$ such that the following diagram commutes:*



A straightforward use of the universal property shows that $S(V)$ is unique up to isomorphism. The existence of symmetric algebras is shown in [DNR01, 4.3.3] with an explicit construction of $S(V)$ as the quotient $T(V)/I$, where

$$I = \langle u \otimes v - v \otimes u : u, v \in V \rangle. \tag{1.10}$$

An alternative construction can be found in [MR01, 15.1.18]. Using (1.9) we have, for all $u, v \in V$,

$$\begin{aligned}
\Delta_{T(V)}(u \otimes v - v \otimes u) &= \Delta(u)\Delta(v) - \Delta(v)\Delta(u) \\
&= (u \otimes 1 + 1 \otimes u)(v \otimes 1 + 1 \otimes v) - (v \otimes 1 + 1 \otimes v)(u \otimes 1 - 1 \otimes u) \\
&= (u \otimes v - v \otimes u) \otimes 1 + 1 \otimes (u \otimes v - v \otimes u) \in I \otimes T(M) + T(M) \otimes I, \\
\varepsilon_{T(V)}(u \otimes v - v \otimes u) &= \varepsilon(u)\varepsilon(v) - \varepsilon(v)\varepsilon(u) = 0, \\
S_{T(V)}(u \otimes v - v \otimes u) &= S(u)S(v) - S(v)S(u) = (-y) \otimes (-x) - (-x) \otimes (-y) \in I,
\end{aligned}$$

meaning that I is a Hopf ideal. Hence, by Example 1.4, $S(V) = T(V)/I$ is a (commutative) Hopf algebra with the induced operations.

EXAMPLE 1.8 (UNIVERSAL ENVELOPING ALGEBRA OF A LIE ALGEBRA). We say that a $\Bbbk$-vector space $\mathfrak{g}$ is a $\Bbbk$-*Lie algebra*, if there exists a $\Bbbk$-bilinear map $[-,-] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, called the *Lie bracket*, such that the following conditions hold:

(L1) (*Antisymmetry*) $[x, y] = -[y, x]$, for all $x, y \in \mathfrak{g}$,

(L2) (*Jacobi identity*) $[[x, y], z] + [[z, x], y] + [[y, z], x] = 0$, for all $x, y, z \in \mathfrak{g}$.

The Lie algebra $\mathfrak{g}$ is called *abelian* if $[x, y] = 0$ for every $x, y \in \mathfrak{g}$.

Notice that, in general, the product $[-,-]$ is not associative. Moreover, (L1) implies $[x, x] = 0$, for all $x \in \mathfrak{g}$. For example, $\mathbb{R}^3$ equipped with the usual vector product is a $\mathbb{R}$-Lie algebra.

Every (associative) $\Bbbk$-algebra A can be endowed with a $\Bbbk$-Lie algebra structure by putting $[a, b] := ab - ba$, for all $a, b \in A$. In this example we shall consider the converse construction,

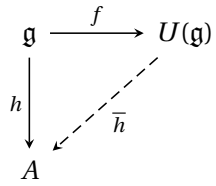
i.e., an associative algebra rising from a Lie algebra given. The importance of these associative algebras is well known, going from representation theory (cf. [Hum72]), construction of Verma modules (cf. [Hal03, §9.5]) or characterization of left-invariant differential operators (cf. [Hel01, Chapter II]), to commutative cases of quantum groups (cf. [Kas95]).

If $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are two $\Bbbk$-Lie algebras, we say that a $\Bbbk$-linear map $f:\mathfrak{g}_1\to\mathfrak{g}_2$ is an *morphism of Lie algebras*, if

$$f([x,y])=[f(x),f(y)],\qquad \text{for all } x,y\in\mathfrak{g}_1.$$

In particular, if $\mathfrak{g}_2=A$ is an associative $\Bbbk$-algebra endowed with the Lie bracket mentioned above, we say that the map $f:\mathfrak{g}_1\to A$ is a *representation* (of $\mathfrak{g}_1$).

Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra. We say that an associative $\Bbbk$-algebra $U(\mathfrak{g})$ is an *universal enveloping algebra of* $\mathfrak{g}$, if there exists a representation $f:\mathfrak{g}\to U(\mathfrak{g})$ such that the following universal property is satisfied: *for any associative $\Bbbk$-algebra A and any representation $h:\mathfrak{g}\to A$ there exists an unique algebra morphism $\overline{h}:U(\mathfrak{g})\to A$ such that the following diagram is commutative:*



From the above follows that $\overline{h}$ is also a $\Bbbk$-Lie morphism and that $U(\mathfrak{g})$ is unique up to isomorphism. The existence of such enveloping algebra is shown in [Kas95, §V.2] and [Lez19c, p. 20] with an explicit construction of $U(\mathfrak{g})$ as the quotient algebra $\Bbbk\langle X\rangle/I$, where $X=\{x_i\}_i$ is a basis of $\mathfrak{g}$, $\Bbbk\langle X\rangle$ is the free $\Bbbk$-algebra over X (cf. Example A.1) and

$$I=\langle x_ix_j-x_jx_i-[x_i,x_j]:x_j,x_i\in X\rangle.$$

An alternative construction of $U(\mathfrak{g})$ can be found in [DNR01, 4.3.4], where $U(\mathfrak{g})$ is defined as the quotient $T(\mathfrak{g})/J$, where $T(\mathfrak{g})$ is the tensor algebra of $\mathfrak{g}$ (cf. Example 1.6) and

$$J=\langle[x,y]-x\otimes y+y\otimes x:x,y\in\mathfrak{g}\rangle. \tag{1.11}$$

Either case, the Poincaré-Birkhoff-Witt Theorem (cf. [Jac79, Theorem V.3]) establishes that, if there exists a total order $\leq$ in X, then the set containing 1 and all elements of the form

$$x_{i_1}\cdots x_{i_n},\qquad \text{with } x_{i_1}\leq\cdots\leq x_{i_n},$$

form a $\Bbbk$-basis of $U(\mathfrak{g})$.

The rules

$$\Delta(x)=x\otimes 1+1\otimes x,\qquad \varepsilon(x)=0\qquad\text{and}\qquad \varepsilon(x)=-x,\qquad\text{for all } x\in\mathfrak{g}, \tag{1.12}$$

can be extended to $U(\mathfrak{g})$; this is done applying the universal property or, alternatively, verifying that J, defined in (1.11), is a Hopf ideal. Either case, (1.12) gives $U(\mathfrak{g})$ a structure of cocommutative $\Bbbk$-Hopf algebra.

EXAMPLE 1.9 (ENVELOPING UNIVERSAL ALGEBRA OF $\mathfrak{sl}_2(\Bbbk)$). Denote by $\mathfrak{gl}_2(\Bbbk)$ the $\Bbbk$-algebra con-

sisting of all $n \times n$ matrices with entries in $\Bbbk$ seen as Lie algebra. One can easily check that

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

form a $\Bbbk$-basis for $\mathfrak{gl}_2(\Bbbk)$. Moreover,

$$[x, y] = h, \qquad [h, x] = 2x, \qquad [h, y] = -2y \qquad \text{and} \qquad [i, x] = [i, y] = [i, h] = 0.$$

We denote by $\mathfrak{sl}_2(\Bbbk)$ the subspace of all matrices with null trace; a basis is $\{x, y, h\}$. For the particular case $\Bbbk = \mathbb{C}$, in [Kas95, Chapter V] a detailed study of this Lie algebra can be found.

By the previous example, $U(\mathfrak{sl}_2(\Bbbk))$ can be seen as a Hopf algebra generated by x, y, h attached to the relation $[x, y] = h$, $[h, x] = 2x$ and $[h, y] = -2y$. In Chapter 2 we will endow this algebra with another structure, evidencing the a single object can be endowed with several distinct structures.

Recall that $\omega \in \Bbbk$ is said to be a *n-th root of unity* ($n \in \mathbb{Z}^+$) if $\omega^n = 1$. Furthermore, ω is *primitive* if it is not a k-th root of unity for some $k < n$.

Example 1.10 (Taft Hopf algebra). Given a n-th root of unity ω in $\Bbbk$, the n^2-dimensional *Taft Hopf algebra* is given as an algebra by

$$T_{n^2}(\omega) = \Bbbk\langle g, x\rangle / I,$$

where $I = \langle g^n - 1, x^n, xg - \omega gx\rangle$. $T_{n^2}(\omega)$ acquires structure of non-(co)commutative Hopf algebra via

$$\begin{aligned} \Delta(g) &= g \otimes g, \qquad \varepsilon(g) = 1, \qquad S(g) = g^{-1}, \\ \Delta(x) &= x \otimes 1 + g \otimes x, \qquad \varepsilon(x) = 0, \qquad S(x) = -g^{-1}x. \end{aligned}$$

Since the construction depends on the choice of ω, there are $\Phi(n)$ non-isomorphic Taft Hopf algebras for each dimension n^2, where Φ denotes Euler's totient function. These Hopf algebras were constructed as an example of finite dimensional Hopf algebra having antipodes of arbitrarily high order, since in $T_{n^2}(\omega)$, S has order $2n$ (cf. [Taf71]). In the case $n = 2$, $T_{2^2}(\omega)$ is also known as the *Sweedler Hopf algebra*.

Example 1.11 (Quantum enveloping algebra of $\mathfrak{sl}_2(\Bbbk)$). Let $q \in \Bbbk$ an invertible element such that $q \neq \pm 1$. We define $U_q := U_q(\mathfrak{sl}_2(\Bbbk))$ as the $\Bbbk$-algebra generated by e, f, k, k^{-1} attached to the relations

$$\begin{gathered} kk^{-1} = k^{-1}k = 1, \qquad kek^{-1} = q^2 e, \qquad kfk^{-1} = q^{-2} f, \\ [e, f] = ef - fe = \frac{k - k^{-1}}{q - q^{-1}}. \end{gathered}$$

It can be shown that $\{e^i f^j k^l : i, j \in \mathbb{N}, l \in \mathbb{Z}\}$ is a basis for this algebra (cf. [Kas95, Proposition VII.1.1]). For simplicity, set $\Bbbk = \mathbb{C}$ and $q \in \mathbb{C}$ not being a root of the unit. Hence U_q is a $\mathbb{C}$-Hopf

algebra with the operations induced by

$$\Delta(e) := 1 \otimes e + e \otimes k, \qquad \Delta(f) := k^{-1} \otimes f + f \otimes 1, \qquad \Delta(k) := k \otimes k, \qquad \Delta(k^{-1}) := k^{-1} \otimes k^{-1},$$
$$\varepsilon(e) = \varepsilon(f) = 0, \qquad \varepsilon(k) = \varepsilon(k^{-1}) = 1,$$
$$S(e) := -ek^{-1}, \qquad S(f) := -kf, \qquad S(k) := k^{-1}, \qquad S(k^{-1}) := k.$$

Moreover, if q^2 is a n-th primitive root of unity, the elements $k^n - 1$, e^n and f^n are skew-primitive. Hence, by [Kha15, Proposition 1.7], the ideal generated by them is a Hopf ideal and thus $U_q' := U_q / \langle k^n - 1, e^n, f^n \rangle$ is a Hopf algebra. U_q' is known as the *Frobenius-Lusztig kernel*.

EXAMPLE 1.12 (CIRCLE HOPF ALGEBRA). Let $H_{\Bbbk}$ be the algebra $H_{\Bbbk} := \Bbbk\langle c, s \rangle / I$, where

$$I = \langle c^2 + s^2 - 1, cs \rangle.$$

$H_{\Bbbk}$ is a Hopf algebra via

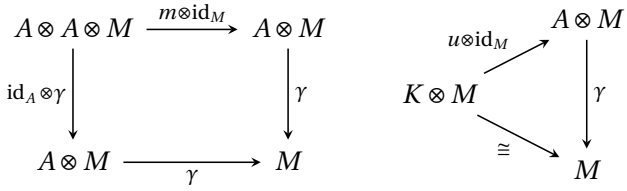
$$\Delta(c) = c \otimes c - s \otimes s, \qquad \varepsilon(c) = 1, \qquad S(c) = c,$$
$$\Delta(s) = c \otimes s + s \otimes c, \qquad \varepsilon(s) = 0, \qquad S(s) = -s.$$

As we shall see in Example 1.3.1.3, this algebra naturally appears in some examples of separable field extensions not being Galois, but still satisfying the Hopf Galois extension property.

1.2 MODULE ALGEBRAS AND COMODULE ALGEBRAS

The aim of this section is to study (co)actions of a Hopf algebra over an arbitrary K-algebra; they are of utmost importance for Hopf Galois extensions. Therefore, we review the notions of (co)module over an algebra and (co)module algebra. Throughout this section A will denote an arbitrary K-algebra, while C a K-coalgebra.

DEFINITION 1.16 (LEFT MODULE OVER AN ALGEBRA, [MON93, DEFINITION 1.6.1]). A *left A-module* is a K-module M together with a K-linear map $\gamma : A \otimes M \to M$, called the *scalar product map* of M, such that the following diagrams are commutative:



Classically, a left module over A would be a K-module M together with a K-bilinear map $A \times M \to M$, denoted by $(a, m) \mapsto a \cdot m$ (or simply am), such that $1 \cdot m = m$ and $(ab) \cdot m = a \cdot (b \cdot m)$, for all $m \in M$ and $a, b \in A$. As expected, our definition is equivalent to the classical one with the identification $\gamma(a \otimes m) := a \cdot m$. Therefore, we will use either notation.

Similarly, *right modules* over A are defined, the difference being that the scalar product map has the form $\gamma : M \otimes A \to M$.

DEFINITION 1.17 (RIGHT COMODULE OVER A COALGEBRA, [MON93, DEFINITION 1.6.2]). A *right C-comodule* is a K-module N together with a K-linear map $\rho : N \to N \otimes C$, called the *structure map* of N, such that the following diagrams are commutative:

$$\begin{array}{ccc} N & \xrightarrow{\rho} & N \otimes C \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_N \otimes \Delta} \\ N \otimes C & \xrightarrow[\rho \otimes \mathrm{id}_C]{} & N \otimes C \otimes C \end{array} \qquad \begin{array}{ccc} N & \overset{\cong}{\searrow} & \\ {\scriptstyle\rho}\downarrow & & N \otimes K \\ N \otimes C & \xrightarrow{\mathrm{id}_N \otimes \varepsilon} & \end{array} \tag{1.13}$$

Left comodules over C are defined similarly, having structure map of the form $\rho : N \to C \otimes N$.

As in coalgebras, calculations with comodules can be tricky. Therefore, we extend Sweedler's sigma notation.

NOTATION (SWEEDLER'S SIGMA NOTATION FOR COMODULES, [MON93, S1.6]). Let N be a right C-comodule with structure map $\rho : N \to N \otimes C$. For any $n \in N$, the element $\rho(n)$ of $N \otimes C$ has the form

$$\rho(n) = \sum_{i=1}^{k} n_{i0} \otimes n_{i1}, \qquad \text{for some } n_{i0} \in N \text{ and } n_{i1} \in C.$$

Extending Sweedler's sigma notation to comodules, we shall rewrite the above as

$$\rho(n) = \sum n_0 \otimes n_1 \qquad \text{or} \qquad \rho(n) = \sum n_{(0)} \otimes n_{(1)},$$

fixing the convention that $n_j \in C$ for $j \neq 0$. With this, the defining properties of a right comodule given in Definition 1.17 may be written as

$$\sum (n_0)_0 \otimes (n_0)_1 \otimes n_1 = \sum n_0 \otimes (n_1)_1 \otimes (n_1)_2 = \sum n_0 \otimes n_1 \otimes n_2, \tag{1.14}$$

$$\sum \varepsilon(n_1) n_0 = n. \tag{1.15}$$

Likewise, if N is a left C-comodule with structure map $\rho : N \to C \otimes N$, preserving the convention for non-zero indexes, we write

$$\rho(n) = \sum n_{-1} \otimes n_0 \qquad \text{or} \qquad \rho(n) = \sum n_{(-1)} \otimes n_{(0)}.$$

Other useful formulas for calculations can be found in [DNR01, §2.1].

DEFINITION 1.18 (MORPHISM OF MODULES, [DNR01, DEFINITION 2.1.9]). Let M, X be two left A-modules, with scalar product maps γ_M and γ_X, respectively. A K-linear map $f : M \to X$ is said to be a *module morphism*, if the following diagram is commutative:

$$\begin{array}{ccc} A \otimes M & \xrightarrow{\mathrm{id}_A \otimes f} & A \otimes X \\ {\scriptstyle\gamma_M}\downarrow & & \downarrow{\scriptstyle\gamma_X} \\ M & \xrightarrow[f]{} & X \end{array}$$

DEFINITION 1.19 (MORPHISM OF COMODULES, [DNR01, DEFINITION 2.1.9]). Let N, L be two right C-comodules, with structure maps ρ_N and ρ_L, respectively. A K-linear map $g : N \to Y$ is said to be a *comodule morphism*, if the following diagram is commutative:

$$\begin{array}{ccc} N & \xrightarrow{g} & Y \\ {\scriptstyle \rho_N}\downarrow & & \downarrow{\scriptstyle \rho_Y} \\ N \otimes C & \xrightarrow[g\otimes \mathrm{id}_C]{} & Y \otimes C \end{array}$$

In this case we also say that g is a *C-colinear map*. In Sweedler's sigma notation,

$$\sum g(n)_0 \otimes g(n)_1 = g(n_0) \otimes n_1, \qquad \text{for all } n \in N.$$

We denote the category of left (resp. right) A-modules by ${}_A\mathrm{Mod}$ (resp. Mod_A). Similarly, the category of right (resp. left) comodules over a coalgebra C is denoted by Mod^C (resp. ${}^C\mathrm{Mod}$). Some result relating these categories can be found in [DNR01, §2.1].

The definition of a bimodule over an algebra can also be dualized.

DEFINITION 1.20 (BIMODULE). Let A, B be two K-algebras. A K-module M is said to be a *B-A-bimodule*, if the following conditions hold:

(BM1) M is a left B-module.

(BM2) M is a right A-module.

(BM3) $(b \cdot m) \cdot a = b \cdot (m \cdot a)$, for all $a \in A$, $b \in B$ and $m \in M$.

If $\gamma : M \otimes A \to M$ and $\alpha : B \otimes M \to M$ are the respective scalar product maps, then (BM3) can be state as $\alpha(\mathrm{id}_B \otimes \gamma) = \gamma(\alpha \otimes \mathrm{id}_A)$. Hence, we can dualize the concept.

DEFINITION 1.21 (BICOMODULE, [DNR01, DEFINITION 2.3.1]). Let C, D be two K-coalgebras. A K-module N is said to be a *D-C-bicomodule*, if the following conditions hold:

(BC1) N is a left D-comodule with structure map $\mu : N \to D \otimes N$,

(BC2) N is a right C-comodule with structure map $\rho : N \to N \otimes C$,

(BC3) $(\mu \otimes \mathrm{id}_C)\rho = (\mathrm{id}_D \otimes \rho)\mu$.

REMARK 7. The compatibility given by (BC3) may be written in Sweedler's sigma notation as

$$\sum (n_0)_{-1} \otimes (n_0)_0 \otimes n_1 = \sum n_{-1} \otimes (n_0)_0 \otimes (n_0)_1, \qquad \text{for all } n \in N.$$

Given two D-C-bicomodules, a *morphism of bicomodules* is a linear map which is both a morphism of left D-comodules and a morphism of right C-modules. Hence, we can define the correspondent category, which is denoted by ${}^D\mathrm{Mod}^C$. Similarly, the category of B-A-bimodules is denoted by ${}_B\mathrm{Mod}_A$.

Now, we define the (co)invariants of a (co)module over a Hopf algebra; they will play a main role in Hopf Galois extensions.

DEFINITION 1.22 (INVARIANTS OF A HOPF ALGEBRA ON A MODULE, [MON93, DEFINITION 1.7.1]). Let H be a Hopf algebra. For a left H-module M, *the set of invariants of H on M* is given by

$$M^H := \{m \in M : h \cdot m = \varepsilon(h)m,\ \forall h \in H\}.$$

DEFINITION 1.23 (COINVARIANTS OF A HOPF ALGEBRA ON A COMODULE, [MON93, DEFINITION 1.7.1]). Let H be a Hopf algebra. For a right H-comodule N with structure map $\rho : N \to N \otimes H$, *the set of coinvariants of H on N* is given by

$$N^{coH} := \{n \in N : \rho(n) = n \otimes 1\}.$$

When $K = \Bbbk$ is a field, a natural question is whether there is a relation between the comodules of H and the modules of the dual Hopf algebra H^* (cf. Example 1.3). The next result shows that, at least in the finite-dimensional case, there exists such a correspondence.

PROPOSITION 1.5 ([MON93, LEMMA 1.7.2]). *Let H be a finite-dimensional $\Bbbk$-Hopf algebra and H^* its dual Hopf algebra. Then, for any $\Bbbk$-vector space N, the following assertions are equivalent:*

(i) *N is a right H-comodule.*

(ii) *N is a left H^*-module.*

Moreover, under these conditions, $N^{H^*} = N^{coH}$.

Proof. Let $\{e_1, \dots, e_n\}$ be a basis for H and $\{e_1^*, \dots, e_n^*\}$ the respective dual basis for H^* (i.e., $e_i^*(e_j) = \delta_{ij}$, the Kronecker delta).

(i)⇒(ii): Let N be a right H-comodule. N becomes a H^*-module via

$$f \cdot n := \sum f(n_1)n_0, \qquad \text{for all } f \in H^*,\ n \in N. \tag{1.16}$$

(ii)⇒(i): Let N be a left H^*-module. N becomes a right H-comodule with structure map $\rho : N \to N \otimes H$ via

$$\rho(a) := \sum_{i=1}^{n} e_i^* \cdot a \otimes e_i. \tag{1.17}$$

We omit the details in these two implications since they are a straightforward verification of the defining conditions. Finally, we have

$$\begin{aligned}
N^{H^*} &= \{n \in N : f \cdot a = u^\circ(f)n,\ \forall f \in H^*\} \\
&= \{n \in N : \textstyle\sum f(n_1)n_0 = (fu)(1_\Bbbk)n, \forall f \in H^*\} \\
&= \left\{n \in N : n_0 \textstyle\sum f(n_1) = f(1_H)n, \forall f \in H^*\right\} \\
&= \left\{n \in N : (\mathrm{id}_N \otimes f)(\rho(n)) = (\mathrm{id}_N \otimes f)(n \otimes 1), \forall f \in H^*\right\} \\
&= \{n \in N : \rho(n) = n \otimes 1\} = N^{coH}.
\end{aligned}$$

□

Now, we review some examples of modules and comodules. They were adapted from [DNR01], [Mon93] and [Mon09].

EXAMPLE 1.13 (ALGEBRAS AND COALGEBRAS). Any K-algebra A is a left module over itself by taking $\gamma_A = m_A$ (in other words, $a \cdot b = ab$, for all $a, b \in A$).

Similarly, any K-coalgebra C is a right comodule over itself by taking $\rho_C = \Delta_C$.

EXAMPLE 1.14 (TENSOR PRODUCT OF MODULES). Let H be a K-Hopf algebra and let V, W be two left H-modules. Then $V \otimes W$ has also structure of left H-module via

$$h \cdot (v \otimes w) := \sum (h_1 \cdot v) \otimes (h_2 \cdot w), \qquad \text{for all } h \in H, v \in V, w \in W.$$

If γ_V and γ_W are the respective structure maps of V and W, the above means that the structure map $\gamma_{V\otimes W}$ is defined as the composition

$$\gamma_{V\otimes W}: \; H \otimes V \otimes W \xrightarrow{\Delta\otimes \mathrm{id}_V \otimes \mathrm{id}_W} H \otimes H \otimes V \otimes W \xrightarrow{\mathrm{id}_H \otimes \tau_{H,V} \otimes \mathrm{id}_W} H \otimes V \otimes H \otimes W \xrightarrow{\gamma_V \otimes \gamma_W} V \otimes W.$$

EXAMPLE 1.15 (TENSOR PRODUCT OF COMODULES). Let H be a K-Hopf algebra and let V, W two right H-comodules with respective structure maps ρ_V and ρ_W. Then $V \otimes W$ is also a right H-comodule by taking $\rho_{V\otimes W}$ as the composition

$$\rho_{V\otimes W}: \; V \otimes W \xrightarrow{\rho_V \otimes \rho_W} V \otimes H \otimes W \otimes H \xrightarrow{\mathrm{id}_V \otimes \tau_{H,W} \otimes \mathrm{id}_H} V \otimes W \otimes H \otimes H \xrightarrow{\mathrm{id}_V \otimes \mathrm{id}_W \otimes m} V \otimes W \otimes H.$$

Using Sweedler's sigma notation for comodules, we have

$$\rho_{V\otimes W}(v \otimes w) = \sum v_0 \otimes w_0 \otimes v_1 w_1, \qquad \text{for all } v \in V,\ w \in W.$$

Just as any Hopf algebra is both an algebra and a coalgebra with certain compatibility, a Hopf module will be both a module and a comodule in which the structure map is a module map.

DEFINITION 1.24 (HOPF MODULE, [MON93, DEFINITION 1.9.1]). Let H be a K-Hopf algebra. A K-module M is said to be a *right H-Hopf module*, if the following conditions hold:

(HM1) M is a right H-module,

(HM2) M is a right H-comodule with structure map $\rho : M \to M \otimes H$,

(HM3) For every $m \in M$ and $h \in H$,

$$\rho(m \cdot h) = \sum (m \cdot h)_0 \otimes (m \cdot h)_1 = \sum m_0 \cdot h_1 \otimes m_1 h_2. \tag{1.18}$$

Notice that (1.18) means that ρ is a H-module morphism, where $M \otimes H$ has the structure of H-module described in Example 1.14.

REMARK 8. In (HM1) we may replace H by a Hopf subalgebra L of H; in such case we say that M is a *right (H, L)-Hopf module*. The category of all right (H, L)-Hopf modules is denoted Mod_L^H, in which morphisms are K-linear maps also being both morphisms of right L-modules and morphisms of right H-comodules. Clearly, changing laterality in Definition 1.24, we may obtain the categories ${}^H\mathrm{Mod}_L$, ${}_L\mathrm{Mod}^H$ and ${}_L^H\mathrm{Mod}$.

Now, we present two remarkable examples of Hopf modules. They are adapted from [DNR01] and [Mon93].

EXAMPLE 1.16 (HOPF ALGEBRAS). Any K-Hopf algebra H is a H-Hopf module via $\rho = \Delta$.

EXAMPLE 1.17 (TRIVIAL HOPF MODULE). Let M be any right H-module. Then $M \otimes H$ is a right H-Hopf module using $\rho = \mathrm{id}_M \otimes \Delta$. An special case of this is when M is the *trivial H-module*, that is, $m \cdot h = \varepsilon(h)m$, for all $m \in M$ and $h \in H$. In this situation, $M \otimes H$ is called the *trivial Hopf module*.

The fundamental theorem of Hopf modules classify all Hopf modules as trivial. The relevance of this result is that it can be applied to determine if a candidate of Hopf module really is it or not.

THEOREM 1.6 (FUNDAMENTAL THEOREM OF HOPF MODULES, [MON93, THEOREM 1.9.4]). *Let M be a right H-Hopf module (that is, $M \in \mathrm{Mod}_H^H$). Then M is isomorphic to $M^{coH} \otimes H$ as right H-Hopf modules, where $M^{coH} \otimes H$ has the trivial structure of Hopf module.*

Finally, we are able to present actions and coactions of any Hopf algebra. Although most results and definition presented are we valid over bialgebras, throughout H will denote an arbitrary K-Hopf algebra flat over K.

DEFINITION 1.25 (MODULE ALGEBRA, [MON93, DEFINITION 4.1.1]). Let A be a K-algebra. We say that A is a *left H-module algebra* (or that H *acts to the left on* A), if the following conditions hold:

(MA1) A is a left H-module.

(MA2) For all $h \in H$ and $a, b \in A$,

$$h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b) \qquad \text{and} \qquad h \cdot 1_A = \varepsilon(h)1_A. \tag{1.19}$$

The next result shows that (MA1) can be restate in terms of the multiplication and unit of A.

PROPOSITION 1.7 ([DNR01, PROPOSITION 6.1.1]). *Let A be a K-algebra. If A is a left H-module then the following assertions are equivalent:*

(i) *A is a left H-module algebra.*

(ii) *The multiplication $m_A : A \otimes A \to A$ and the unit $u_A : K \to A$ are both morphisms of H-modules.*

Proof. Recall that $A \otimes A$ is also a left H-module (cf. Example 1.15). If γ_A is the scalar product map of A, then m_A is a morphism of H-modules if and only if the diagram

$$\begin{array}{ccc} H \otimes A \otimes A & \xrightarrow{\mathrm{id}_H \otimes m_A} & H \otimes A \\ \downarrow{\scriptstyle \gamma_{A\otimes A}} & & \downarrow{\scriptstyle \gamma_A} \\ A \otimes A & \xrightarrow[m_A]{} & A \end{array}$$

commutes, meaning that for every $h \in H$ and $a, b \in A$ we have

$$m_A\gamma_{A\otimes A}(h\otimes a\otimes b) = \left[\gamma_A(\mathrm{id}_H \otimes m_A)\right](h\otimes a\otimes b). \tag{1.20}$$

Expanding the left side we get

$$m_A\gamma_{A\otimes A}(h\otimes a\otimes b) = m_A\left(\sum (h_1\cdot a)\otimes(h_2\cdot b)\right) = \sum (h_1\cdot a)(h_2\cdot b).$$

On the other hand, right side of (1.20) gives

$$\left[\gamma_A(\mathrm{id}_H \otimes m_A)\right](h\otimes a\otimes b) = \gamma_A(h\otimes(ab)) = h\cdot(ab).$$

Comparing, we conclude that m_A is a morphism of H-modules if and only if the left equality of (1.19) holds. A similar argument applies for u_A. □

Now, we dualize Definition 1.25 and Proposition 1.7.

DEFINITION 1.26 (COMODULE ALGEBRA, [MON93, DEFINITION 4.1.1]). Let A be a K-algebra. We say that A is a *right H-comodule algebra* (or that *H coacts to the right on A*), if the following conditions hold:

(CA1) A is a right H-comodule with structure map $\rho : A \to A\otimes H$.

(CA2) For all $a, b \in A$,

$$\rho(ab) = \sum a_0b_0\otimes a_1b_1 \qquad \text{and} \qquad \rho(1_A) = 1_A\otimes 1_H. \tag{1.21}$$

PROPOSITION 1.8 ([DNR01, PROPOSITION 6.1.4]). *Let A be a K-algebra. If A is a right H-comodule then the following assertions are equivalent:*

(i) *A is a right H-comodule algebra.*

(ii) *The multiplication $m_A : A\otimes A \to A$ and the unit $u_A : K \to A$ are both morphisms of H-comodules.*

(iii) *ρ is a K-algebra morphism.*

Proof. (i)⇔(ii): m_A is a morphism of H-comodules if and only if the diagram

$$\begin{array}{ccc} A\otimes A & \xrightarrow{\quad m_A \quad} & A \\ {\scriptstyle \rho_{A\otimes A}}\downarrow & & \downarrow{\scriptstyle \rho_A} \\ A\otimes A\otimes H & \xrightarrow[m_a\otimes \mathrm{id}_H]{} & A\otimes H \end{array}$$

is commutative, meaning that, for any $a, b \in A$, we have

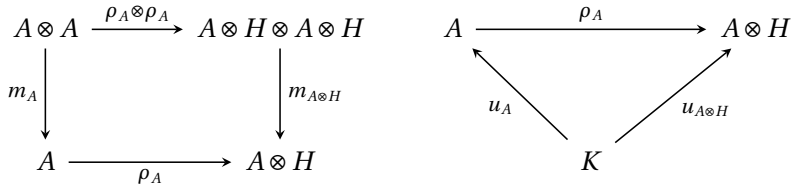
$$\rho_A m_A(a\otimes b) = \left[(m_A\otimes id_H)\rho_{A\otimes A}\right](a\otimes b). \tag{1.22}$$

With the operation behaving as described in Example 1.15, we expand the left side of (1.22) to obtain

$$\left[(m_A \otimes id_H)\rho_{A\otimes A}\right](a\otimes b) = (m_A\otimes id_H)\left(\sum a_0\otimes b_0\otimes a_1 b_1\right) = \sum a_0 b_0 \otimes a_1 b_1.$$

Since $\rho_A m_A(a\otimes b) = \rho_A(ab)$, we have shown the left side of (1.21). Therefore m_A is a morphism of H-comodules if and only if the left relation of (1.21) holds. An analogous argument proves the assertion for u_A.

(i)$\Leftrightarrow$(iii): ρ_A is a morphism of K-algebras if and only if the diagrams



are commutative. Left one means, for $a, b \in A$, that

$$\left[m_{A\otimes H}(\rho_A\otimes\rho_A)\right](a\otimes b) = (\rho_A m_A)(a\otimes b). \tag{1.23}$$

Right side of (1.23) is simply $\rho(ab)$, while the left side is

$$\left[m_{A\otimes H}(\rho_A\otimes\rho_A)\right](a\otimes b) = m_{A\otimes H}\left(\sum a_0\otimes a_1\otimes b_0\otimes b_1\right) = \sum a_0 b_0\otimes a_1 b_1$$

(cf. Example 1.2). We have obtained the left side of (1.21) and therefore it is equivalent to the left diagram. An analogous argument with the right diagram gives right side of (1.21). □

Similarly to the previous definitions, one can have the notion of *right H-module algebra, left H-comodule algebra* and *L-H-bicomodule algebra.*

The next result extends Proposition 1.5.

PROPOSITION 1.9 ([MON09, P. 6.3.9]). *Let H be a finite-dimensional $\Bbbk$-Hopf algebra and H^* its dual Hopf algebra. Then, for a $\Bbbk$-algebra A, the following assertions are equivalent:*

(i) *A is a right H-comodule algebra.*

(ii) *A is a left H^*-module algebra.*

Moreover, under these conditions $A^{H^*} = A^{coH}$.

Proof. Let $\{e_1,\dots,e_n\}$ be a basis for H and $\{e_1^*,\dots,e_n^*\}$ the respective dual basis for H^*.

(i)$\Rightarrow$(ii): Let A be a right H-comodule algebra. We know already that A is a H^*-module via (1.16). Moreover, if $a, b \in A$ and $f \in H^*$, we have

$$\begin{aligned} f\cdot(ab) &= \sum f((ab)_1)(ab_0) = \sum f(a_1b_1)a_0b_0 = \sum (f m_H)(a_1\otimes b_1)a_0b_0 = \sum \Delta^\circ(f)(a_1\otimes b_1)a_0b_0 \\ &= \sum f_1(a_1)f_2(b_1)a_0b_0 = f_1(a_1)a_0 f_2(b_1)b_0 = \sum (f_1\cdot a)(f_2\cdot b); \\ f\cdot 1_A &= f(1_A)1_A = (f u_H)(1_H)1_A = u^\circ(f)1_A. \end{aligned}$$

Therefore, A is a left H^*-module algebra.

(ii)⇒(i): Conversely, let A be a left H^*-module algebra. We know already that A is a H-comodule via (1.17). Moreover, if $a,b \in A$ and $f \in H^*$, we have

$$\begin{aligned}(\mathrm{id}_A \otimes f)(\rho(ab)) &= \sum_{i=1}^{n} e_i^* \cdot (ab) \otimes f(e_i) = \sum_{i=1}^{n} (e_i^* \cdot (ab)) f(e_i) \otimes 1 = \sum_{i=1}^{n} (e_i^* f(e_i)) \cdot (ab) \otimes 1 \\ &= \sum_{i=1}^{n} f \cdot (ab) \otimes 1 = \sum (f_1 \cdot a_1)(f_2 \cdot a_2) \otimes 1 = \sum_{i,j=1}^{n} ((e_i^* f_1(e_i)) \cdot a)((e_j^* f_2(e_j)) \cdot b) \otimes 1 \\ &= \sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes f_1(e_i) f_2(e_j) = \sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes f(e_i e_j) \\ &= (\mathrm{id}_A \otimes f)\left(\sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes e_i e_j \right) = (\mathrm{id}_A \otimes f)(\rho(a)\rho(b)),\end{aligned}$$

and hence $\rho(ab) = \rho(a)\rho(b)$. On the other hand,

$$\rho(1) = \sum_{i=1}^{n} e_i^* \cdot 1_A \otimes e_i = \sum_{i=1}^{n} e_i^*(1_H) 1_A \otimes e_i = \sum_{i=1}^{n} 1_A \otimes e_i^*(1_H) e_i = 1_A \otimes \sum_{i=1}^{n} e_i^*(1_H) e_i = 1_A \otimes 1_H.$$

Thus, A is a right H-comodule algebra.

The equality $A^{H^*} = A^{coH}$ follows as in the proof of Proposition 1.5. □

Now, we generalize Remark 8.

DEFINITION 1.27 (A-H-HOPF MODULES, [SCH90B]). Let A be a right H-comodule algebra. A K-module M is said to be a *Hopf module in* ${}_A\mathrm{Mod}^H$ (or an *A-H-Hopf module*), if the following conditions hold:

(i) M is a left A-module.

(ii) M is a right H-comodule with structure map $\rho_M : M \to M \otimes H$.

(iii) For every $a \in A$ and $m \in M$,

$$\rho_M(am) = \sum a_0 m_0 \otimes a_1 m_1.$$

As expected, the collection of all A-H-Hopf modules, ${}_A\mathrm{Mod}^H$, is a category with morphisms being all K-linear maps which are also A-linear and H-colinear morphisms.

Similarly, objects in the category Mod_A^H can be define with the compatibility being $\rho_M(ma) = \sum m_0 a_0 \otimes m_1 a_1$.

The next result shows that the set of coinvariants in a comodule algebra is always a subalgebra, called the *subalgebra of coinvariants*.

LEMMA 1.10. *Let A is a right H-comodule algebra. Then A^{coH} is a subalgebra of A.*

Proof. If $a, b \in A^{coH}$, then $\rho(a) = a \otimes 1$ and $\rho(b) = b \otimes 1$. Therefore

$$\rho(a+b) = \rho(a) + \rho(b) = a \otimes 1 + b \otimes 1 = (a+b) \otimes 1, \tag{1.24}$$

$$\rho(ka) = k\rho(a) = k(a \otimes 1) = ka \otimes 1, \tag{1.25}$$

$$\rho(ab) = ab \otimes 1. \tag{1.26}$$

Notice that for (1.24) and (1.25) we used the linearity of ρ, while for (1.26) we used (1.21). □

We end this section by giving some examples characterizing actions and coactions of remarkable Hopf algebras. They are adapted from [DNR01], [Mon93] and [Mon09].

EXAMPLE 1.18 (ACTIONS AND COACTIONS OF A HOPF ALGEBRA OVER ITSELF). By Proposition 1.8, H is a right H-comodule algebra using $\rho = \Delta$. By Proposition 1.9, when H if finite dimensional, this dualizes to a left action (denoted by $\rightharpoonup$) of H^* on H given by

$$f \rightharpoonup h = \sum f(h_2)h_1, \qquad \text{for all } h \in H \text{ and } f \in H^*.$$

The (co)invariants are given by $H^{H^*} = H^{coH} = K1$.

EXAMPLE 1.19 (ACTIONS OF THE GROUP ALGEBRA). Let G be a group. We say that G *acts (to the left) as automorphisms* on a $\Bbbk$-algebra A, if there is a group morphism $\psi : G \to \mathrm{Aut}\, A$. In this case we write $\psi(g)(a) = g(a)$ (or $g \cdot a$), for all $g \in G$ and $a \in A$. Moreover, if ψ is injective, we say that G acts *faithful*.

If G acts as automorphisms on a A and $\Bbbk G$ is the group algebra of G (cf. Example 1.5), then A is a left $\Bbbk G$-module algebra via

$$g \cdot a = g(a), \qquad \text{for all } g \in G,\ a \in A.$$

Indeed, for every $g \in G$ and $a, b \in A$, we have

$$g \cdot (ab) = g(ab) = g(a)g(b) = (g \cdot a)(g \cdot b),$$
$$g \cdot 1_A = g(1_A) = 1_A = 1_A 1_A = \varepsilon(g)1_A.$$

In this case, $A^{\Bbbk G}$ is the set of fixed points under the action of G,

$$A^{\Bbbk G} = A^G := \{a \in A : g(a) = a,\ \forall g \in G\}.$$

Conversely, if A is a $\Bbbk G$-module algebra, then G acts as automorphisms on A via $\psi : G \to \mathrm{Aut}\, A$, given by

$$\psi(g)(a) = g \cdot a, \qquad \text{for all } g \in G,\ a \in A.$$

Thus, we have shown that A is a $\Bbbk G$-module algebra if and only if G acts as automorphisms on A.

EXAMPLE 1.20 (COACTIONS OF THE GROUP ALGEBRA). Let G be a group and let A be a $\Bbbk$-algebra. We say that A is a *G-graded algebra* if there exists a collection $\{A_g\}_{g \in G}$ of $\Bbbk$-subspaces of A such that

$$A = \bigoplus_{g \in G} A_g \qquad \text{and} \qquad A_g A_h \subseteq A_{gh}, \text{ for all } g, h \in G.$$

If A is a $\Bbbk G$-comodule algebra with structure map $\rho : A \to A \otimes \Bbbk G$, we replace the Sweedler's sigma notation for

$$\rho(a) = \sum a_g \otimes g, \qquad \text{for all } a \in A.$$

Left diagram of (1.13) gives us

$$[(\mathrm{id}_A \otimes \Delta)\rho](a) = [(\rho \otimes \mathrm{id}_{\Bbbk G})\rho](a), \qquad \text{for all } a \in A.$$

Expanding the left side we get

$$[(\mathrm{id}_A \otimes \Delta)\rho](a) = (\mathrm{id}_A \otimes \Delta)\left(\sum a_g \otimes g\right) = \sum a_g \otimes g \otimes g, \tag{1.27}$$

while right side gives us

$$[(\rho \otimes \mathrm{id}_{\Bbbk G})\rho](a) = (\rho \otimes \mathrm{id}_{\Bbbk G})\left(\sum a_g \otimes g\right) = \sum (a_g)_h \otimes h \otimes g. \tag{1.28}$$

Comparing (1.27) and (1.28) we have that

$$(a_g)_h = \begin{cases} a_g & \text{if } g = h, \\ 0 & \text{if } g \neq h. \end{cases}$$

Thus $\rho(a_g) = a_g \otimes g$ and we can set $A_g = \{a_g : a \in A\}$, for all $g \in G$. Since ρ is a $\Bbbk$-linear map, we have $\rho(a+b) = \rho(a) + \rho(b)$ and $\rho(ka) = k\rho(a)$, for all $a, b \in A$ and $k \in \Bbbk$. Thus,

$$(a+b)_g = a_g + b_g \qquad \text{and} \qquad (ka)_g = ka_g,$$

and therefore A_g is a $\Bbbk$-subspace of A, for all $g \in G$. On the other hand, since G is a basis of $\Bbbk G$, the sum $\sum_{g \in G} A_g$ is direct. Indeed, if $0 = a_{g_1} + \cdots + a_{g_t}$ for some $a_{g_k} \in A_{g_k}$, $1 \leq k \leq t$, by applying ρ we get

$$0 \otimes 0 = \rho(0) = \rho(a_{g_1} + \cdots + a_{g_t}) = \rho(a_{g_1}) + \cdots + \rho(a_{g_t}) = a_{g_1} \otimes g_1 + \cdot + a_{g_t} \otimes g_t,$$

and thus $a_{g_k} = 0$, $1 \leq k \leq t$. Additionally, since A is a $\Bbbk G$-comodule algebra,

$$\rho(a_g b_h) = a_g b_h \otimes gh, \text{for all } a_g \in A_g,\ b_h \in A_h.$$

Therefore $a_g b_h \in A_{gh}$ and $A_g A_h \subseteq A_{gh}$. Finally, right side of (1.13) gives us

$$[(\mathrm{id}_A \otimes \varepsilon)\rho](a) = a \otimes 1, \qquad \text{for all } a \in A.$$

But left side is

$$[(\mathrm{id}_A \otimes \varepsilon)\rho](a) = (\mathrm{id}_A \otimes \varepsilon)\left(\sum a_g \otimes g\right) = \sum a_g \otimes 1,$$

and thus for each $a \in A$, we have $\sum a_g = a$. Therefore $A = \bigoplus_{g \in G} A_g$ and A is a G-graded algebra. Notice that

$$A^{coH} = \{a \in A : \rho(a) = a \otimes 1\} = A_1,$$

the identity component of the G-graduation. In particular, $1_A \in A_1$.

Conversely, if A is a G-graded algebra set the structure map $\rho : A \to A \otimes \Bbbk G$ by

$$\rho(a) = a \otimes g, \qquad \text{for all } a \in A_g.$$

With this, we have shown that A is a $\Bbbk G$-comodule algebra if and only if A is a G-graded algebra.

EXAMPLE 1.21 (ACTIONS OF THE DUAL GROUP ALGEBRA). Let G be a finite group and $H = (\Bbbk G)^*$. By the universal property of $\Bbbk G$, we can identify H with $\Bbbk^G$, the algebra of functions from G to $\Bbbk$. Thus, for $f, g \in \Bbbk^G$ and $x, y \in G$, and with the notation of Example 1.3,

$$\begin{gathered}(f \cdot g)(x) := [m^\circ(f \otimes g)](x) = [\Delta^*(f \otimes g)](x) = [(f \otimes g)\Delta](x) = (f \otimes g)(x \otimes x) = f(x)g(x),\\ [\Delta(f)](x) := [\Delta^\circ(f)](x \otimes y) = [m^*(f)](x \otimes y) = f(xy),\\ [S(f)](x) := [S^\circ(f)](x) = [S^*(f)](x) = [fS](x) = f(S(x)).\end{gathered}$$

Despite this formulas, a full description of $\Delta(f)$ is not given. Therefore we define, for every $x \in G$, the map $p_x : G \to \Bbbk$ given by

$$p_x(y) := \delta_{x,y} := \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

Since G is finite, $\{p_x : x \in G\}$ is a basis for $\Bbbk^G$ (in correspondence with the dual basis of $(\Bbbk G)^*$). For those elements, we have

$$\Delta(p_x) = \sum_{uv=x} p_u \otimes p_v = \sum_{y \in G} p_y \otimes p_{y^{-1}x}.$$

By Proposition 1.9, actions of $\Bbbk^G$ correspond to coactions of $\Bbbk G$, which by Example 1.20 are precisely G-gradings.

EXAMPLE 1.22 (ACTIONS OF THE UNIVERSAL ENVELOPING ALGEBRA OF A LIE ALGEBRA). Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $U(\mathfrak{g})$ its universal enveloping algebra (cf. Example 1.8). If A is a $U(\mathfrak{g})$-module algebra, since for every $x \in \mathfrak{g}$, $\Delta(x) = x \otimes 1 + 1 \otimes x$ and $\varepsilon(x) = 0$, using (1.19) we get

$$x \cdot (ab) = x \cdot (a)b + a(x \cdot b) \qquad \text{and} \qquad x \cdot 1 = 0.$$

Hence, $A^{U(\mathfrak{g})} := A^{\mathfrak{g}} = \{a \in A : x \cdot a = 0, \text{ for all } x \in \mathfrak{g}\}$.

1.3 HOPF GALOIS EXTENSIONS

Finally, we are able to introduce one of the transversal concepts to this document. Hopf Galois extensions generalize the notion of Galois extensions over rings, replacing the action of a group on the algebra by the coaction of a Hopf algebra. The first general definition is due to [KT81], although the commutative case was studied in [CS69].

DEFINITION 1.28 (RIGHT HOPF GALOIS EXTENSION, [MON93, DEFINITION 8.1.1]). Let A be a right H-comodule algebra with structure map $\rho : A \to A \otimes H$. We say that the extension $A^{coH} \subset A$

(also denoted A/A^{coH}) is a *right H-Galois extension*, if the map $\beta : A \otimes_{A^{coH}} A \to A \otimes_K H$, given by

$$\beta(a \otimes b) = (a \otimes 1)\rho(b) = \sum ab_0 \otimes b_1, \qquad \text{for all } a, b \in A, \tag{1.29}$$

is bijective. In this case β is called the *Galois map*.

As a first remark, notice that we could have defined the Galois map $\beta' : A \otimes_{A^{coH}} A \to A \otimes_K H$ as

$$\beta'(a \otimes b) = \rho(a)(b \otimes 1) = \sum a_0 b \otimes a_1, \qquad \text{for all } a, b \in A. \tag{1.30}$$

A natural question is whether β' can replace β. The next result gives a case in which the answer is affirmative.

PROPOSITION 1.11 ([KT81, PROPOSITION 1.2]). *Let A be a right H-comodule algebra with structure map $\rho : A \to A \otimes H$. If the antipode S is bijective, then the following assertions are equivalent:*

(i) *The map β, given by (1.29), is bijective (resp. injective, surjective).*

(ii) *The map β', given by (1.30), is bijective (resp. injective, surjective).*

Proof. Let $\Phi : A \otimes H \to A \otimes H$ the endomorphism given by

$$\Phi(a \otimes h) := \rho(a)(1 \otimes S(h)) = \sum a_0 \otimes a_1 S(h), \qquad \text{for all } a \in A,\ h \in H.$$

We have, for all $a, b \in A$,

$$\begin{aligned}(\Phi\beta)(a \otimes b) &= \Phi\left(\sum ab_0 \otimes b_1\right) = \sum \Phi(ab_0 \otimes b_1) = \sum \rho(ab_0)(1 \otimes S(b_1)) \\ &= \sum (a_0 b_0 \otimes a_1 b_1)(1 \otimes S(b_2)) = \sum a_0 b_0 \otimes a_1 b_1 S(b_2) = \sum a_0 b_0 \otimes a_1 \varepsilon(b_1) \\ &= \sum a_0 b_0 \varepsilon(b_1) \otimes a_1 = \sum a_0 b \otimes a_1 = \beta'(a \otimes b).\end{aligned}$$

Hence $\Phi\beta = \beta'$. But notice that Φ has as inverse $\Phi^{-1} : A \otimes H \to A \otimes H$ given by

$$\Phi^{-1}(a \otimes h) := (1 \otimes S^{-1}(h))\rho(a) = \sum a_0 \otimes S^{-1}(h) a_1, \qquad \text{for all } a \in A,\ h \in H.$$

Therefore the assertions are equivalent. □

Left H-Galois extensions can be defined similarly, having Galois map $\beta_l : A \otimes_{A^{coH}} A \to H \otimes_{\Bbbk} A$.

NOTATION. If several Hopf Galois extensions of different laterality are involved, we add to their Galois maps an index indicating whether they are left or right sided; for example, for a right Hopf Galois extension we may write β_r.

A particular case of interest in Hopf Galois extension theory is when the subalgebra of coinvariants coincides with the base ring K.

DEFINITION 1.29 (RIGHT HOPF GALOIS OBJECT, [CS69]). When a right H-Galois extension is of the form $K \subset A$ (i.e., $A^{coH} = K$), we called A a *right H-Galois object*.

REMARK 9. Notice that, in this situation, the Galois map β is given by the composition

$$\beta\colon\ A\otimes A \xrightarrow{\mathrm{id}_A\otimes\rho_A} A\otimes A\otimes H \xrightarrow{m_A\otimes\mathrm{id}_H} A\otimes H.$$

PROPOSITION 1.12 ([CS69, THEOREM 1.15]). *Let A be a right H-Galois object. Then A is a faithfully flat K-module.*

As bimodules or bialgebras, the setup of Galois objects can be bilateral with certain compatibility.

DEFINITION 1.30 (HOPF BIGALOIS OBJECT, [SCH96, DEFINITION 3.4]). Let H, L be two K-Hopf algebras. A K-algebra A is said to be a *L-H-biGalois object* if the following assertions hold:

(BG1) A is a faithfully flat L-H-bicomodule algebra.

(BG2) A is a left L-Galois extension of K.

(BG3) A is a right H-Galois extension of K.

1.3.1 EXAMPLES

We review some examples of Hopf Galois extensions. Most of them are adapted from [DNR01], [Mon93], [Mon09] and [Sch04].

1.3.1.1 HOPF ALGEBRAS

Every K-Hopf algebra H can be seen as a K-Galois object. Indeed, since H has a natural structure of H-comodule algebra via the comultiplication (i.e., the structure map is $\rho := \Delta$), for any $h \in H^{coH}$,

$$\rho(h) = \Delta(h) = \sum h_1 \otimes h_2 = h \otimes 1.$$

Applying $\varepsilon \otimes \mathrm{id}_H$ we have

$$(\varepsilon\otimes\mathrm{id}_H)\left(\sum h_1\otimes h_2\right) = (\varepsilon\otimes\mathrm{id}_H)(h\otimes 1) \qquad \Rightarrow \qquad \sum \varepsilon(h_1)1\otimes h_2 = \varepsilon(h)1\otimes 1,$$

which via the isomorphism $K\otimes H \cong H$, gives

$$h = \sum \varepsilon(h_1)h_2 = \varepsilon(h)1.$$

That is, $h \in K$. Conversely, if $h \in K$ then $\Delta(h) = \Delta(h1) = h\Delta(1) = h(1\otimes 1) = h\otimes 1$ and therefore $h \in H^{coH}$. Hence $H^{coH} = K$.

The map $\beta : H\otimes H \to H\otimes H$ is defined by

$$\beta(a\otimes b) = (a\otimes 1)\rho(b) = (a\otimes 1)\Delta(b) = \sum ab_1\otimes b_2, \qquad \text{for all } a,b\in H.$$

Then, the inverse $\beta^{-1} : H\otimes H \to H\otimes H$ of the Galois map is given by

$$\beta^{-1}(a\otimes b) = \sum aS(b_1)\otimes b_2, \qquad \text{for all } a,b\in H.$$

Indeed, if $a, b \in H$, then

$$\begin{aligned}\beta(\beta^{-1}(a\otimes b)) &= \beta\left(\sum aS(b_1)\otimes b_2\right) = \sum \beta(aS(b_1)\otimes b_2) = \sum aS(b_1)b_2\otimes b_3\\ &= \sum a\varepsilon(b_1)\otimes b_2 = \sum a\otimes \varepsilon(b_1)b_2 = a\otimes b;\\ \beta^{-1}(\beta(a\otimes b)) &= \beta^{-1}\left(\sum ab_1\otimes b_2\right) = \sum \beta^{-1}(ab_1\otimes b_2) = \sum ab_1S(b_2)\otimes b_3\\ &= \sum a\varepsilon(b_1)\otimes b_2 = \sum a\otimes \varepsilon(b_1)b_2 = a\otimes b.\end{aligned}$$

Therefore β is bijective and we have shown the next result.

PROPOSITION 1.13 ([DNR01, EXAMPLE 6.4.8]). *Let H be a K-Hopf algebra. Then $K \subset H$ is a H-Galois extension.*

REMARK 10. Since Hopf Galois extensions are definable over bialgebras, it can be shown for every bialgebra H that, in fact, H is a Hopf algebra if and only if $K \subset H$ is a H-Galois extension (cf. [Sch04, Example 2.1.2]). More generally, if H is a K-flat bialgebra admitting a H-Galois extension $A^{coH} \subset A$ that is faithfully flat as K-module, H must be a Hopf algebra (cf. [Sch97]).

1.3.1.2 CLASSICAL FIELD EXTENSIONS

Let G be a finite group acting as automorphisms on a field $E \supset \Bbbk$ in the sense of Example 1.19. Obviously E is a $\Bbbk$-algebra. Moreover, we know that E is a left $\Bbbk G$-module algebra. Hence, by Proposition 1.9, it is a right $\Bbbk^G$-comodule algebra ($(\Bbbk G)^* = \Bbbk^G$, cf. Example 1.21).

As the name suggest, the next result shows that classical Galois extensions of fields can be seen as Hopf Galois extensions.

THEOREM 1.14 ([MON93, 8.1.2]). *Let G be a finite group acting as automorphisms on a field $E \supset \Bbbk$, and $F := E^G$. Then the following assertions are equivalent:*

(i) *The field extension $E \subset F$ is Galois with Galois group G.*

(ii) *G acts faithfully on E.*

(iii) $[E : F] = |G|$.

(iv) *$F \subset E$ is a right $\Bbbk^G$-Galois extension.*

Proof. The implications (i)⇔(ii)⇔(iii) are consequence of Artin's Lemma (cf. [Jac85, Theorem 4.7] or [Hun74, Theorem V.2.15]). Hence, we will just show their equivalence with (iv). Suppose that the field extension $F \subset E$ is Galois. Set $n := |G|$ and $G = \{x_1, \dots, x_n\}$. Let $\{u_1, \dots, u_n\}$ be a basis of E/F and let $\{p_1, \dots, p_n\} \subset \Bbbk^G$ be the dual basis to $\{x_i\} \subset \Bbbk G$. As said before, E coacts on $\Bbbk^G$, where the structure map $\rho : E \to E \otimes \Bbbk^G$ is given by

$$\rho(a) = \sum_{i=1}^{n} (x_i \cdot a) \otimes p_i, \qquad \text{for all } a \in E.$$

Therefore, the Galois map $\beta : E \otimes_F E \to E \otimes_{\Bbbk} \Bbbk^G$ is given by

$$\beta(a \otimes b) = (a \otimes 1)\rho(b) = \sum_{i=1}^{n} a(x_i \cdot b) \otimes p_i.$$

We must prove that β is bijective. For that, suppose $w = \sum_j a_j \otimes u_j \in \ker(\beta)$. Then

$$\beta(w) = \sum_j a_j(x_i \cdot u_j) \otimes p_i = 0 \otimes 0.$$

Since the p_i are linearly independent, we conclude that

$$\sum_j a_j(x_i \cdot u_j) = 0, \qquad \text{for all } 1 \leq i \leq n. \tag{1.31}$$

Using the faithfulness of the action of G, Dedekind independence theorem gives that the $n \times n$ matrix $C = [x_i \cdot u_j]$ associated to the system (1.31) is invertible (cf. [Jac85, p. 291]). Hence all a_j are 0 and $w = 0$. Thus β is injective. Since both $E \otimes_F E$ and $E \otimes_{\Bbbk} \Bbbk^G$ are F-vector spaces of dimension n^2, if follows that β is a bijection.

Conversely, suppose that the Galois map β is an isomorphism. Notice that

$$\dim_F(E \otimes_F E) = [E : F]^2 \qquad \text{and} \qquad \dim_F(E \otimes_{\Bbbk} \Bbbk^G) = [E : F]|G|.$$

Via the isomorphism, we get $[E : F] = |G|$ and therefore $F \subset E$ is a Galois extension of fields. □

1.3.1.3 SEPARABLE FIELD EXTENSIONS

For the circle Hopf algebra $H_{\Bbbk}$ (cf. Example 1.12), it is possible for a finite separable field extension $F \subset F$ to be $H_{\Bbbk}$-Galois, although it is not Galois in the classical sense. This example is due to [GP87].

Let $\Bbbk = F = \mathbb{Q}$ and $E = F(\omega)$, where ω is the real 4-th root of 2. $F \subset E$ is not Galois for any group G, since the automorphism group of E/F fixes $\mathbb{Q}(\sqrt{2})$ pointwise. However, if $H_{\mathbb{Q}}$ is the circle Hopf algebra, it can be shown that $F \subset E$ is $H_{\mathbb{Q}}^*$-Galois; in this case $H_{\mathbb{Q}}$ acts on E as follows:

$\cdot$	1	ω	ω^2	ω^3
c	1	0	$-\omega^2$	0
s	0	$-\omega$	0	ω^3

When we change $\Bbbk$ for $\mathbb{Q}(i)$, $H_{\Bbbk} \cong \Bbbk\mathbb{Z}_4$, the group algebra of $\mathbb{Z}_4$; that is $\mathbb{Q}\mathbb{Z}_4$ and $H_{\mathbb{Q}}$ are $\mathbb{Q}(i)$-forms of each other. For a suitable Hopf algebra H, which is a $\mathbb{Q}(\sqrt{-2})$-form of $\mathbb{Q}[\mathbb{Z}_2 \times \mathbb{Z}_2]$, $\mathbb{Q} \subset E$ is also a H^*-Galois (cf. [Par90, §3]). Hence an extension can be Hopf Galois over two different Hopf algebras.

1.3.1.4 STRONGLY GRADED ALGEBRAS

Let $A = \bigoplus_{g \in G} A_g$ be a G-graded algebra (cf. Example 1.20). A is said to be *strongly graded* if $A_g A_h = A_{gh}$, for all $g, h \in G$.

LEMMA 1.15 ([NVO04, PROPOSITION 1.1.1]). *Let A be a G-graded algebra. Then the following assertions are equivalent:*

(i) *A is strongly graded,*

(ii) *$A_g A_{g^{-1}} = A_1$ for all $g \in G$.*

Proof. (i)⇒(ii) is trivial. (ii)⇒(i): We have

$$A_{gh} = A_{gh}A_1 = A_{gh}(A_{h^{-1}}A_h) \subseteq (A_{gh}A_h^{-1})A_h \subseteq A_{ghh^{-1}}A_h = A_g A_h \subseteq A_{gh},$$

for all $g, h \in G$. □

Recall that A is a $\Bbbk G$-comodule algebra with structure map $\rho : A \to A \otimes \Bbbk G$ given by

$$\rho(a) = a \otimes g, \qquad \text{for all } a \in A_g,$$

and that $A^{co\Bbbk G} = A_1$. Notice that $\beta : A \otimes_{A_1} A \to A \otimes_{\Bbbk} \Bbbk G$ is given by

$$\beta(a \otimes b) = (a \otimes 1)\rho(b) = \sum_{g \in G} ab_g \otimes g, \qquad \text{for all } a, b \in A \text{ with } b = \sum_{g \in G} b_g.$$

The next theorem is due to Ulbrich and Osterburg (cf. [vU81]).

THEOREM 1.16 ([MON93, THEOREM 8.1.7]). *Let G be any (multiplicative) group and let A be a G-graded algebra. Then the following assertions are equivalent:*

(i) *$A_1 \subset A$ is a $\Bbbk G$-extension.*

(ii) *A is strongly graded.*

Proof. (i)⇒(ii) First assume that β is bijective and, in particular, surjective. Whence for every $g \in G$ there exists finitely many $a_i, b_i \in A$ such that

$$\beta\left(\sum_i a_i \otimes b_i\right) = \sum_i \sum_{h \in G} a_i (b_i)_h \otimes h = \sum_{i,h} a_i (b_i)_h \otimes h = 1 \otimes g.$$

Since G is a basis for $\Bbbk G$, it follows that $\sum_i a_i (b_i)_g = 1$ and $\sum_i a_i (b_i)_h = 0$ for all $h \neq g$. The inclusion $A_g A_{g^{-1}} \subseteq A_1$ always holds in a G-graded algebra; so now suppose $a \in A_1$. Fixing g, we have $a = a1 = a\sum_i a_i (b_i)_g = \sum_i a a_i (b_i)_g$. Since $(b_i)_g$ are homogeneous of degree g, a is homogeneous of degree 1 and the sum of homogeneous components is direct, we get $a_i \in A_{g^{-1}}$. Hence $A_g A_{g^{-1}} = A_1$ and by Lemma 1.15 it follows that A is strongly graded.

(ii)⇒(i): Conversely, suppose now that A is strongly graded. If $g \in G$, then by Lemma 1.15, $1 \in A_1 = A_{g^{-1}} A_g$ and we may write $1 = \sum_i a_i b_i$ for some $a_i \in A_{g^{-1}}$ and $b_i \in A_g$. Therefore let $\alpha : A \otimes_{\Bbbk} \Bbbk G \to A \otimes_{A_1} A$ be defined as

$$\alpha(a \otimes g) = \sum_i a a_i \otimes b_i.$$

Since all $g_i \in A_g$, we get

$$(\beta\alpha)(a\otimes g) = \beta\left(\sum_i aa_i\otimes b_i\right) = \sum_i aa_ib_i\otimes g = a(a_ib_i)\otimes g = a1\otimes g = a\otimes g.$$

On the other hand,

$$(\alpha\beta)(a\otimes b) = \alpha\left(\sum_{g\in G} ab_g\otimes g\right) = \sum_{g\in G}\alpha(ab_g\otimes g) = \sum_{g\in G}\sum_i ab_ga_i\otimes b_i,$$

but $b_ga_i \in A_gA_{g^{-1}} = A_1$ and hence

$$(\alpha\beta)(a\otimes b) = \sum_{g\in G}\sum_i ab_ga_i\otimes b_i = \sum_{g\in G}\sum_i a\otimes b_ga_ib_i = \sum_{g\in G} a\otimes b_g\left(\sum_i a_ib_i\right) = \sum_{g\in G} a\otimes b_g1 = a\otimes b.$$

Therefore $\alpha = \beta^{-1}$ and β is bijective. □

1.3.1.5 CROSSED PRODUCTS OVER GROUPS

We now give a major example that can be deduce from the previous one. Let G be a (multiplicative) group acting as automorphisms on a $\Bbbk$-algebra R; we denoted the action by $g(r) = g\cdot r$. The action is said to be *twisted* if there exists a map $\sigma : G\times G\to R$ such that the following conditions hold:

(i) (*Cocycle condition*) For all $g,h,k\in G$,

$$[g\cdot\sigma(h,k)]\sigma(h,hk) = \sigma(g,h)\sigma(gh,k),$$
$$\sigma(g,1) = \sigma(1,g) = 1.$$

(ii) (*Twisted module condition*) For all $g,h\in G$ and $r\in R$,

$$[g\cdot(h\cdot r)]\sigma(g,h) = \sigma(g,h)(gh\cdot r).$$

In this case, we say that σ is a *2-cocycle*.

We define a new different structure over $R\otimes\Bbbk G$; in this context, an arbitrary element $r\otimes g$ of $R\otimes\Bbbk G$ will be denoted by $r*g$.

DEFINITION 1.31 (CROSSED PRODUCT OVER A GROUP, [MON09, EXAMPLE 2.7]). Let G be a (multiplicative) group acting as automorphisms on a $\Bbbk$-algebra R. If the action is twisted, we define the *crossed product of R and G*, denoted by $R*G$, as the $\Bbbk$-space $R\otimes\Bbbk G$ together with the multiplication

$$(r*g)(s*h) = r(g\cdot s)\sigma(g,h)*gh, \qquad \text{for all } r,s\in R \text{ and } g,h\in G,$$

and unit element 1_R*1_G.

PROPOSITION 1.17 ([MON09, EXAMPLE 2.7]). *Let G be a (multiplicative) group acting as automorphisms on a $\Bbbk$-algebra R. Suppose that the action is twisted. Then $R*G$ is a G-graded algebra. Moreover, $R \subset A$ is a $\Bbbk G$-Galois extension.*

Proof. For all $g,h,k \in G$ and $r,s,t \in R$ we have

$$\begin{aligned}(r*g)[(s*h)(t*k)] &= (r*g)(s(h\cdot t)\sigma(h,k)*hk) = r\left[g\cdot(s(h\cdot t)\sigma(h,k))\right]\sigma(g,hk)*g(hk)\\ &= r\left[(g\cdot s)(g\cdot(h\cdot t))(g\cdot\sigma(h,k))\right]\sigma(g,hk)*g(hk)\\ &= r(g\cdot s)(g\cdot(h\cdot t))\left[(g\cdot\sigma(h,k))\sigma(g,hk)\right]*(gh)k\\ &= r(g\cdot s)(g\cdot(h\cdot t))\left[\sigma(g,h)\sigma(gh,k)\right]*(gh)k\\ &= r(g\cdot s)\left[(g\cdot(h\cdot t))\sigma(g,h)\right]\sigma(gh,k)*(gh)k\\ &= r(g\cdot s)\left[\sigma(g,h)(gh\cdot t)\right]\sigma(gh,k)*(gh)k\\ &= \left[r(g\cdot s)\sigma(g,h)*gh\right](t*k) = \left[(r*g)(s*h)\right](t*k).\end{aligned}$$

On the other hand,

$$\begin{aligned}(r*g)(1*1) &= r(g\cdot 1)\sigma(g,1)*g1 = r1*g1 = r*g,\\ (1*1)(r*g) &= 1(1\cdot r)\sigma(1,g)*1g = 1r1*1g = r*g.\end{aligned}$$

Hence, $R*G$ is a $\Bbbk$-algebra. The homogeneous components are given by

$$(R*G)_1 = R\otimes 1 \cong R \qquad \text{and} \qquad (R*G)_g = R\otimes g, \quad \text{for all } g\in G.$$

Finally, since $(R*G)_g(R*G)_h = R\otimes gh = (R*G)_{gh}$, for all $g,h\in G$, the algebra is strongly graded and therefore, by Theorem 1.16, $R\subset A$ is $\Bbbk G$-Galois. □

The relation between crossed products over groups and group extensions is explored in [Mon09, Example 2.8], showing that for any group G with normal subgroup N and quotient $L = G/N$, $\Bbbk G = \Bbbk N * \Bbbk L$. Also, in [Mon09, Examples 2.9 and 2.10], counterexamples of strongly graded algebras that are not crossed products are given.

1.3.1.6 HOPF CROSSED PRODUCTS AND SMASH PRODUCTS

In a more general setting, let H be a K-Hopf algebra and R a H-module algebra. The action is said to be *twisted*, if there exists a map $\sigma : H\times H \to R$ such that the following conditions hold:

(i) (*Hopf 2-cocycle condition*) For all $g,h,k\in H$,

$$\sum [g_1\cdot\sigma(h_1,k_1)]\sigma(g_2,h_2k_2) = \sum \sigma(g_1,h_1)\sigma(g_2h_2,k), \tag{1.32}$$

$$\sigma(g,1) = \sigma(1,g) = \varepsilon(g)1. \tag{1.33}$$

(ii) (*Hopf twisted module condition*) For all $g,h\in H$ and $r\in R$,

$$[g\cdot(h\cdot r)] = \sum \sigma(g_1,h_1)(g_2h_2\cdot r)\sigma(g_3,h_3)^{-1}. \tag{1.34}$$

In this case, we say that σ is a *2-cocycle*.

DEFINITION 1.32 (HOPF CROSSED PRODUCT, [MON09, EXAMPLE 3.6]). Let H be a K-Hopf algebra and R a H-module algebra. If the action is twisted, we define the *crossed product of R and H*, denoted by $R\#_\sigma H$, as the K-module $R\otimes H$ together with the multiplication

$$(r\#g)(s\#h)=\sum r(g_1\cdot s)\sigma(g_2,h_1)\#g_3h_2,\qquad \text{for all } r,s\in R \text{ and } g,h\in H, \tag{1.35}$$

and unit element $1_R\#1_H$.

For any group G, if $H=\Bbbk G$, this definition coincides with that of a crossed product over G. Other particular examples can be found in [Mon93, Chapter 7].

THEOREM 1.18 ([MON09, EXAMPLE 3.6]). *Let R a H-module algebra. Suppose that the action is twisted. If $A:=R\#_\sigma H$, then:*

(i) *A is an algebra.*

(ii) *A is a right H-comodule algebra via $\rho: A\to A\otimes H$ given by*

$$\rho(r\#h)=\sum(r\#h_1)\otimes h_2,\qquad \textit{for all } r\#h\in A.$$

(iii) $A^{coH}\cong R$.

Proof. (i) For all $r,s,t\in R$ and $g,h,f\in H$, we have

$$\begin{aligned}
(r\#g)\left[(s\#h)(t\#f)\right] &= (r\#g)\left[\sum s(h_1\cdot t)\sigma(h_2,f_1)\#h_3f_2\right]\\
&= \sum r(g_1\cdot(s(h_1\cdot t)\sigma(h_2,f_1)))\sigma(g_2,(h_3f_2)_2)\#g_3(h_3f_2)_2\\
&= \sum r(g_1\cdot(s(h_1\cdot t)\sigma(h_2,f_1)))\sigma(g_2,h_4f_3)\#g_3h_4f_3\\
&\overset{(1.19)}{=} \sum r(g_1\cdot s)(g_2\cdot(h_1\cdot t))(g_3\cdot\sigma(h_2,f_1))\sigma(g_4,h_4f_3)\#g_5h_4f_3\\
&\overset{(1.32)}{=} \sum r(g_1\cdot s)(g_2\cdot(h_1\cdot t))\sigma(g_3,h_2)\sigma(g_4h_3,f_1)\#g_5h_4f_2\\
&\overset{(1.34)}{=} \sum r(g_1\cdot s)\sigma(g_2,h_1)(g_3h_2\cdot t)\sigma(g_4h_3,f_1)\#g_5h_4f_2\\
&= \sum r(g_1\cdot s)\sigma(g_2,h_1)((g_3h_2)_1\cdot t)\sigma((g_3h_2)_2,f_2)\#(g_3h_2)_3f_2\\
&= \left[\sum r(g_1\cdot s)\sigma(g_2,h_1)\#g_3h_2\right](t\#f)=\left[(r\#g)(s\#h)\right](t\#f)
\end{aligned}$$

and

$$\begin{aligned}
(r\#g)(1\#1)=\sum r(g_1\cdot 1)\sigma(g_2,1)\#g_3 &\overset{(1.34)}{=} \sum(g_1\cdot 1)\varepsilon(g_2)\#g_3\\
&\overset{(1.19)}{=} \sum\varepsilon(g_1)\varepsilon(g_2)\#g_3=\sum r\#\varepsilon(g_1g_2)g_3=r\#g,\\
(1\#1)(r\#g)=\sum 1(1\cdot r)\sigma(1,g_1)\#1g_2 &\overset{(1.34)}{=} \sum r\varepsilon(g_1)\#g_2=\sum r\#\varepsilon(g_1)g_2=r\#g.
\end{aligned}$$

Therefore, $R\#_\sigma H$ is an algebra.

(ii) Since for all $r \in R$ and $h \in H$ we have

$$\begin{aligned}
[(\mathrm{id}_{R\#_\sigma H} \otimes \Delta)\rho](r\#h) &= (\mathrm{id}_{R\#_\sigma H} \otimes \Delta)\left(\sum (r\#h_1) \otimes h_2\right) = \sum (a\#h_1) \otimes h_2 \otimes h_3 \\
&= (\rho \otimes \mathrm{id}_H)\left(\sum (r\#h_1) \otimes h_2\right) = [(\rho \otimes \mathrm{id}_H)\rho](r\#h), \\
[(\mathrm{id}_{R\#_\sigma H} \otimes \varepsilon)\rho](r\#h) &= (\mathrm{id}_{R\#_\sigma H} \otimes \varepsilon)\left(\sum (r\#h_1) \otimes h_2\right) = \sum (r\#h_1) \otimes \varepsilon(h_2)1 = r\#h_1\varepsilon(h_2) \otimes 1 = r\#h \otimes 1,
\end{aligned}$$

it follows that $R\#_\sigma H$ is an H-module. Moreover, for all $r, s \in R$ and $g, h \in H$,

$$\begin{aligned}
\rho((r\#g)(s\#h)) &= \rho\left(\sum r(g_1 \cdot s)\sigma(g_2, h_1)\#g_3h_2\right) = \sum (r(g_1 \cdot s)\sigma(g_2, h_1)\#(g_3h_2)_1) \otimes (g_3h_2)_2 \\
&= \sum (r(g_1 \cdot s)\sigma(g_2, h_1)\#g_3h_2 \otimes g_4h_3 = \sum (r\#g_1)(s\#h_1) \otimes g_2h_2, \\
\rho(1 \otimes 1) &= (1\#1) \otimes 1,
\end{aligned}$$

meaning that $R\#_\sigma H$ is an H-comodule algebra.

(iii) We have

$$(R\#_\sigma H)^{coH} = \left\{z \in R\#_\sigma H : \rho(z) = z \otimes 1\right\}.$$

Clearly, $R \cong R\#_\sigma 1 \subseteq (R\#_\sigma H)^{coH}$; reciprocally, if $r\#h \in (R\#_\sigma H)^{coH}$, applying $\mathrm{id}_R \otimes \varepsilon \otimes \mathrm{id}_H$ to the equality $\rho(r\#h) = (r\#h) \otimes 1$ we get in the left

$$(\mathrm{id}_R \otimes \varepsilon \otimes \mathrm{id}_H)(\rho(r\#h)) = (\mathrm{id}_R \otimes \varepsilon \otimes \mathrm{id}_H)\left(\sum (r\#h_1) \otimes h_2\right) = \sum (r\#\varepsilon(h_1)1) \otimes h_2 = (r\#1) \otimes h,$$

while in the right

$$(\mathrm{id}_R \otimes \varepsilon \otimes \mathrm{id}_H)((r\#h) \otimes 1) = (r\#\varepsilon(h)1) \otimes 1 = (r\#1) \otimes \varepsilon(h)1.$$

Comparing, we get that $h = \varepsilon(h)1 \in K$ and hence $r\#h = r\varepsilon(h)\#1 \in R\#_\sigma 1 \cong R$. Hence, $A^{coH} \cong R$, as wanted. □

Hopf crossed products are relevant since they characterize Hopf Galois extensions having the normal basis property (cf. [Mon09, Theorem 3.8]).

A particular case of Hopf crossed products is when the cocycle σ is *trivial*, that is, when $\sigma(g, h) = \varepsilon(g)\varepsilon(h)$ for all $g, h \in H$. In this case we write $R\#H$ and the multiplication (1.35) is simply

$$(r\#g)(s\#h) = \sum r(g_1 \cdot s)\#g_2h, \qquad \text{for all } r, s \in R \text{ and } g, h \in H.$$

$R\#H$ is called the *smash product* of R and H.

Under these conditions, Theorem 1.18 restates as follows.

THEOREM 1.19. *Let R be a H-module algebra. Then $A := R\#H$ is a H-comodule algebra with structure map $\rho : A \to A \otimes H$ given by*

$$\rho(r\#h) = \sum (r\#h_1) \otimes h_2, \qquad \textit{for all } r \in R \textit{ and } h \in H.$$

Moreover, $A^{coH} \cong R$.

COROLLARY 1.20 ([DNR01, EXAMPLE 6.4.3]). *Let R be a H-module algebra. Then $R \subset R\#H$ is a H-Galois extension.*

Proof. We have $\beta : (R\#H) \otimes_R (R\#H) \to (R\#H) \otimes H$ defined as $\beta(z \otimes w) = (z \otimes 1)\rho(w)$, for all $z, w \in R\#H$. But since the first tensor is taken over $R\#1 \cong R$, for all $r, s \in A$ and $h, g \in H$ we have $(r\#h)(s\#1) \otimes (1\#g) = (r\#h) \otimes (s\#g)$. Thus, is enough to study β on elements of the form $(r\#h) \otimes (1\#g)$. That is,

$$\begin{aligned}\beta((r\#h) \otimes (1\#g)) &= ((r\#h) \otimes 1)\rho(1\#g) = ((r\#h) \otimes 1)\left(\sum (1\#g_1) \otimes g_2\right) \\ &= \sum ((r\#h)(1\#g_1)) \otimes g_2 = \sum (r(h_1 \cdot 1)\#h_2 g_1) \otimes g_2 = \sum (r\varepsilon(h_1)\#h_2 g_1) \otimes g_2 \\ &= \sum (r\#hg_1) \otimes g_2.\end{aligned}$$

As in the proof of Proposition 1.13, the inverse $\beta^{-1} : (R\#H) \otimes H \to (R\#H) \otimes_R (R\#H)$ is given by

$$\beta^{-1}((r\#h) \otimes g) = \sum (r\#hS(g_1)) \otimes (1\#g_2), \qquad \text{for all } r \in R \text{ and } h, g \in H.$$

Indeed, if $r \in R$ and $h, g \in H$, we have

$$\begin{aligned}\beta^{-1}(\beta((r\#h) \otimes (1\#g))) &= \beta^{-1}\left(\sum (r\#hg_1) \otimes g_2\right) = \sum (r\#hg_1 S((g_2)_1)) \otimes (1\#(g_2)_2) \\ &= \sum (r\#hg_1 S(g_2)) \otimes (1\#g_3) = \sum (r\#h\varepsilon(g_1)) \otimes (1\#g_2) \\ &= (r\#h) \otimes (1\#g), \\ \beta(\beta^{-1}((r\#h) \otimes g)) &= \beta\left(\sum (r\#hS(g_1)) \otimes (1\#g_2)\right) = \sum (r\#hS(g_1)(g_2)_1) \otimes (g_2)_2 \\ &= \sum (r\#hS(g_1)g_2) \otimes g_3 = \sum (r\#h\varepsilon(g_1)) \otimes g_2 \\ &= (r\#h) \otimes g.\end{aligned}$$

Therefore, $R \subset R\#H$ is a H-Galois extension. □

Smash products are relevant for Hopf Galois extensions, since when H is finite dimensional, a generator of their category of modules describes all H^*-Galois extensions (cf. Theorem 1.32).

1.3.1.7 GROUPS ACTING ON SETS

The Galois map β can be seen as the dual of a natural map arising whenever a group acts on a set, as shows this example. Recall that if G is a (multiplicative) group and X is a non-empty set, a function $\mu : X \times G \to X$ is called a *(right) group action of G on X*, which we denote by $(x, g) \mapsto x \cdot g$, if

$$x \cdot 1 = x \qquad \text{and} \qquad x \cdot (gh) = (x \cdot g) \cdot h, \qquad \text{for all } x \in X \text{ and } g, h \in G.$$

The action is said to be *free* if for a given $g \in G$ such that $x \cdot g = x$, for some $x \in X$, it follows that $g = 1$; in other words, no element in G, besides 1, has fixed points. It is not hard to check that an action is free if and only if, given $g, h \in G$, the existence of an $x \in X$ such that $x \cdot g = x \cdot h$ implies $g = h$.

Also, recall that for any $x \in X$, its *orbit* is defined by $x \cdot G := \{x \cdot g : g \in G\}$; the set of all orbits of X under the action of G is denoted by X/G and is called the *quotient* of the action.

Consider the map $\alpha : X \times G \to X \times X$ given by $(x, g) \mapsto (x, x \cdot g)$. Notice that α is injective if

only if the action is free. Moreover, the image of this map can bee seen as a pull-back. Indeed,

$$\begin{aligned}\mathrm{Im}(\alpha) &= \{(x,y) \in X \times X : y = x \cdot g \text{ for some } g \in G\} \\ &= \{(x,y) \in X \times X : x \cdot G = y \cdot G\} \\ &= X \times_{X/G} X,\end{aligned}$$

called *the fiber product* of X with itself over X/G via the canonical surjective map $x \mapsto x \cdot G$.

We want to dualize this scenario; for simplicity assume that X and G are finite. We denote by $A := \Bbbk^X$ the algebra of functions from X to $\Bbbk$ endowed with the pointwise addition and multiplication; the unit of this algebra is the map $1_A : X \to \Bbbk$ given by $x \mapsto 1_\Bbbk$. We say that $a \in A$ is *constant on G-orbits* if $a(x \cdot g) = a(x)$, for all $x \in X$ and $g \in G$; the set of functions constant on G-orbits is denoted by $\Bbbk^{X/G}$. Finally, recall that $H := (\Bbbk G)^* = \Bbbk^G$ is the Hopf algebra of function from G to $\Bbbk$ (cf. Example 1.21). Hence, we have the following.

LEMMA 1.21 ([MON93, EXAMPLE 8.1.9]). *Let X be a finite non-empty set, G a finite group and $\mu : X \times G \to X$ a right group action. If $A = \Bbbk^X$ and $H = \Bbbk^G$, then:*

(i) *The right G-action on X induces a left G-action on A, given by $(g \cdot a)(x) := a(x \cdot g)$,*

(ii) *A is a right H-comodule algebra with induced structure map $\mu^* : A \to A \otimes H$. Moreover, $A^{coH} = \Bbbk^{X/G}$.*

Proof. (i) For every $a \in A$, $g, h \in G$ and $x \in X$ we have

$$\begin{aligned}(1 \cdot a)(x) &= a(x \cdot 1) = a(x), \\ ((gh) \cdot a)(x) &= a(x \cdot (gh)) = a((x \cdot g) \cdot h) = (h \cdot a)(x \cdot g) = (g \cdot (h \cdot a))(x).\end{aligned}$$

(ii) Since for any non-empty sets U and V, $\Bbbk^{U \times V} \cong \Bbbk^U \otimes \Bbbk^V$, we have $A \otimes H \cong \Bbbk^{X \otimes G}$. Thus, we can define $(\mu^*(a))(x,g) = a\mu(x,g) = a(x \cdot g)$. The verification of A being a right H-comodule algebra is straightforward. It is evident that $A^{coH} = \Bbbk^{X/G}$. □

The map α defined above dualizes to $\alpha^* : A \otimes_B A \to A \otimes_\Bbbk H$; by transposition, it is given by

$$\alpha^*(a \otimes b) = (a \otimes 1)\mu^*(b), \qquad \text{for all } a, b \in A. \tag{1.36}$$

That is, $\alpha^* = \beta$, the Galois map. By remarks in previous paragraphs, the freeness of the action is equivalent to $\Bbbk^{X/G} \subset \Bbbk^X$ being a $\Bbbk^G$-Galois extension. In other words, we have the following.

THEOREM 1.22 ([MON93, EXAMPLE 8.1.9]). *Let X be a finite non-empty set, G a finite group and $\mu : X \times G \to X$ a right group action. The Galois map $\beta = \alpha^*$ given by (1.36) is bijective if and only if $\alpha : X \times G \to X \times_{X/G} X$ is bijective if and only if the G-action is free.*

1.3.1.8 ALGEBRAIC GROUP SCHEMES

Recall that a $\Bbbk$-algebra A is called *affine*, if it is finitely generated as $\Bbbk$-algebra, i.e., there exist finitely many elements $a_1, \ldots, a_n \in A$ such that every element of A can be expressed as a poly-

nomial in $a_1, \ldots, a_n$ with coefficients in $\Bbbk$. This definition we use is the one given by [Mon93, Definition 4.2.3]; however, nowadays in most contexts affine algebras are also required to be commutative and reduced (i.e., without nilpotent elements).

We say that X is an *affine scheme* if $X = \mathrm{Spec}(A)$ for a commutative affine $\Bbbk$-algebra A. Similarly, G is said to be an *affine algebraic group scheme* if $G = \mathrm{Spec}(H)$ for some commutative affine $\Bbbk$-Hopf algebra H. As in Lemma 1.21, any action $\mu : X \times G \to X$ is determined by a coaction $\rho = \mu^* : A \to A \otimes_\Bbbk H$.

LEMMA 1.23 ([MON09, EXAMPLE 2.12]). *Let $X = \mathrm{Spec}(A)$ be an affine scheme, $G = \mathrm{Spec}(H)$ an affine algebraic group scheme and $\rho : A \to A \otimes_\Bbbk H$ a coaction. The map $\alpha : X \times G \to X \times X$ given by*

$$\alpha(x, g) = (x, x \cdot g), \qquad \text{for all } x, \in X \text{ and } g \in G,$$

is a closed embedding if and only if $\alpha^* : A \otimes_\Bbbk A \to A \otimes_\Bbbk H$ given by

$$\alpha^*(a, b) = (a \otimes 1)\rho(b)$$

is surjective. Under these conditions we say that the coaction ρ is free.

However, in contrast with the previous example, the Galois map can not be α^*, since its domain is not $A \otimes_{A^{coH}} A$. Instead, we shall proceed differently by applying the Spec functor to the exact sequence

$$A^{coH} \hookrightarrow A \underset{-\otimes 1}{\overset{\rho}{\rightrightarrows}} A \otimes_{A^{coH}} A,$$

and geting an exact sequence of affine schemes

$$X \times G \underset{\pi}{\overset{\mu}{\rightrightarrows}} X \longrightarrow \mathrm{Spec}(A^{coH}),$$

where π is the projection of the first coordinate. $\mathrm{Spec}(A^{coH})$ is called the *affine quotient* of X by G.

In general, $Y := \mathrm{Spec}(A^{coH})$ not necessarily coincides with X/G, the set of G-orbits on X (cf. [Mon09, Example 2.12]). However, if the coaction is free, it will happen that $Y = X/G$; thus the map $X \times G \to X \times_Y X$ is an isomorphism and $X \to Y$ is faithfully flat. In an algebraic sense, we have the following result.

THEOREM 1.24 ([MON09, EXAMPLE 2.12]). *Let $X = \mathrm{Spec}(A)$ be an affine scheme, $G = \mathrm{Spec}(H)$ an affine algebraic group scheme and $\rho : A \to A \otimes_\Bbbk H$ a free coaction. Then,*

(i) *$\beta : A \otimes_{A^{coH}} A \to A \otimes_\Bbbk H$ is bijective and so $B \subset A$ is H-Galois,*

(ii) *A is a faithfully flat A^{coH}-module.*

1.3.1.9 PRINCIPAL BUNDLES

In this example we discuss why, in non-commutative algebraic geometry, faithfully flat Hopf Galois extensions are considered a generalization of classical affine principal bundles. Our

main reference for this is [BF12]. Let us first shortly recall some basic terminology related to topological bundles.

DEFINITION 1.33 (BUNDLE, [BF12, DEFINITION 1]). A *bundle* is a triple (E,π,M) where E and M are topological spaces an $\pi : E \to M$ is a continuous surjective map.

Here M is called the *base space*, E the *total space* and π the *projection* of the bundle. For each $m \in M$, the *fibre* over m is the topological space $E_m := \pi^{-1}(m)$. A *local section* of a bundle is a continuous map $s : U \to E$ with $\pi s = \mathrm{id}_M|_U$, where U is an open subset of M. If each fibre of a bundle is endowed with a vector space structure such that the addition and scalar multiplication are continuous, we call it a *vector bundle*.

When the fibers of a bundle are all homeomorphic to a common space F, it is known as a *fibre bundle*. Intuitively, an example of fibre bundle is the Möbius strip, since it has a circle that runs lengthwise through the center of the strip as a base M and a line segment running vertically for the fibre F. The line segments are in fact copies of the real line, so $F = \mathbb{R}$.

REMARK 11. Commonly, in the definition of fibre bundle a condition of local triviality is asked for π, which means that, for each $x \in E$, there is a open neighborhood $U_x \subset M$ and a homeomorphism $\phi_x : \pi^{-1}(U_x) \to U_x \times F$ such that the following diagram commutes:

$$\begin{array}{ccc} \pi^{-1}(U_x) & \xrightarrow{\phi_x} & U_x \times F \\ \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle p_1} & \\ U_x & & \end{array}$$

Here p_1 denotes the first projection.

REMARK 12. In the most general sense, a *bundle* over an object M in a category $\mathscr{C}$ is a morphism $\pi : E \to M$ in $\mathscr{C}$. For $m : 1 \to M$, a generalized element of M, the *fibre* E_m is defined as the pullback of E along m.

Given an object F in $\mathscr{C}$, $p : E \to M$ is called a *fibre bundle* with standard fibre F, if given any $m : 1 \to M$, E_m is isomorphic to F. Locally trivial fibre bundles can be defined over sites (cf. [Hus94, p. 20]).

Let X be a topological space and G a topological group. Suppose there is a right action $\mu : X \times G \to X$ and write $\mu(x,g) = x \cdot g$. We had seen in previous examples that, even without structure, G acts freely on X if and only if the map $\alpha : X \times G \to X \times X$, given by $(x,g) \mapsto (x, x \cdot g)$, is injective if and only if $\alpha : X \times G \to X \times_{X/G} X$ is bijective. Furthermore, $(X,\pi,X/G)$ is a bundle, where π is the natural projection.

Recall that a continuous map $f : Y \to W$ is *proper* if the map $f \times \mathrm{id}_Z : Y \times Z \to W \times Z$ is closed, for any topological space Z. The action μ is said to be *proper* if it is continuous and $\alpha : X \times G \to X \times X$ is proper.

DEFINITION 1.34 (PRINCIPAL BUNDLE, [BHMS06, DEFINITION 1.15]). A *G-principal bundle* is a quadruple (X,π,M,G) such that

(i) (X,π,M) is a bundle and G is a topological group acting continuously on X from the right

via $\mu : X \times G \to X$,

(ii) μ is principal (i.e., free and proper),

(iii) $\pi(x) = \pi(y)$ if and only if there exists $g \in G$ such that $y = x \cdot g$,

(iv) The induced map $X/G \to M$ is a homeomorphism.

The first two properties tell us that principal bundles are bundles admitting a principal action of a group G on the total space X, i.e., principal bundles correspond to principal actions. But, by previous remarks, those are just continuous free actions (i.e., continuous actions such that $\alpha : X \times G \to X \times X$ is injective). The third property ensures that the fibres of the bundle correspond to the orbits coming from the action and the final one implies that the quotient space can topologically be viewed as the base space of the bundle.

The next two examples are due to [BHMS06, p. 13] and [BF12, p. 4].

EXAMPLE 1.23. Clearly, a principal right action of G on X automatically makes the bundle $(X, \pi, X/G)$ a G-principal bundle. However, not every principal bundle has to be of this form. If we replace X/G by a homeomorphic space, not only we formally define a different bundle, but also it might happen that such a new bundle is not equivalent to $(X, \pi, X/G)$ (cf. [Fri00, p. 157]).

EXAMPLE 1.24. Any vector bundle can be understood as a bundle associated to a principal bundle in the following way: consider a G-principal bundle (X, π, M, G) and let V be a *representation space* of G, that is, a (topological) vector space with a (continuous) left G-action $G \times V \to V$, denoted $(g, v) \mapsto g \cdot v$. Then G acts from the right on $X \times V$ by

$$(x, v) \cdot g := (xg, g^{-1} \cdot v), \qquad \text{for all } x \in X,\ v \in V \text{ and } g \in G.$$

Hence, we define $E = (X \times V)/G$ and a surjective (continuous) map $\pi_E : E \to M$ given by

$$(x, v)G \mapsto \pi(x), \qquad \text{for all } x \in X,\ v \in V.$$

Thus we have a fibre bundle (E, π_E, M, V).

More examples can be found in [Coh98, §1.2].

REMARK 13. In a category $\mathscr{C}$, given a group object G, a *G-principal bundle* (also called a *G-torsor*) is a bundle $\pi : E \to X$ equipped with a G-action $\mu : E \times G \to G$ on E over X such that the canonical morphism $\alpha : E \times G \to E \times_X E$ is an isomorphism, which in turn means that the action is free and transitive over X and hence each fiber of the bundle looks like G once we choose a base point.

In other words, this says that, after picking any point of X as the identity, X "acquires a group structure" isomorphic to G. Hence, colloquially, a torsor is understood as a group that has forgotten its identity.

In specific contexts (as that of the category of topological spaces, in Definition 1.34), several perspectives for torsors come up. For example:

- In the category of sets, a G-torsor over a set X becomes a group action $X \times G \to G$ (denoted by $(x, g) \to x \cdot g$) such that for any $x_1, x_2 \in X$, there exists a unique $g \in G$ such that $x_1 \cdot g = x_2$.

Usually g is denoted by x_2/x_1 and is called the *ratio* of x_1 and x_2. Due to the above, notice that, while in an multiplicative (resp. additive) group G one can multiply and divide (resp. add and subtract) elements, in a G-torsor one can multiply (resp. add) an element of G to an element of X and get a result in X, or one can divide (resp. subtract) two elements of X and get a result in G.
Basic examples of torsors are the anti-derivatives of a function or the euclidean plane without the origin (cf. Section 1.4). There are more elaborated ones in physics; namely, differences of energy, differences of voltage, the relative phases in quantum mechanics, etc. A great explanation of these can be found in [Bae09].

- In algebraic geometry, given a smooth algebraic group G, a G-torsor over a scheme X is a scheme with an action of G that is locally trivial in the given Grothendieck topology (cf. [Ols16]).
- Recent works in measurement theory attempt to understand the algebraic structure underlying the quantity calculus as topological bundles (cf. [Dom17, Rap18]).

Sticking with topological bundles, we want to dualize the setup in order to obtain a non-commutative version. For simplicity, assume that X is a complex affine variety with an action of an affine algebraic group G and set $Y = X/G$ with the usual Euclidean topology. Let $A := \mathcal{O}(X)$, $B := \mathcal{O}(Y)$ and $H := \mathcal{O}(G)$ be the corresponding coordinate rings. Since $\mathcal{O}(G \times G) \cong \mathcal{O}(G) \otimes \mathcal{O}(G)$, H is a Hopf algebra with operations given by

$$\Delta(f)(g,h) = f(gh), \qquad \varepsilon(f) = f(e) \qquad \text{and} \qquad (Sf)(g) = f(g^{-1}).$$

Using the fact that G acts on X from the right, A is a right H-algebra comodule with structure map $\rho : A \to A \otimes H$ given by $\rho(a)(x,g) := a(x \cdot g)$ (cf. [BF12, p. 5]). Notice that B can be viewed as a subalgebra of A via $\pi^* : B \to A$ given by $b \mapsto b \circ \pi$, where π is the canonical surjection $\pi : X \to X/G$. Indeed, the map π^* is injective since $b \neq b'$ in $B = \mathcal{O}(X/Y)$ means that there exists at least one orbit $x \cdot G$ such that $b(x \cdot G) \neq b'(x \cdot G)$. But, since $\pi(x) = x \cdot G$, it follows $\pi^*(b) \neq \pi^*(b')$.

Furthermore, $a \in \pi^*(B)$ if and only if $a(x \cdot g) = a(x)$, for all $x \in X$ and $g \in G$, meaning that $\rho(a)(x,g) = (a \otimes 1)(x,g)$, where $1 : G \to \mathbb{C}$ is the unit function $1(g) = 1$. Hence $a \in A^{coH}$. The other inclusion is obvious, so $A^{coH} = \pi^*(B) \cong B$.

Finally, notice that we can identify $\mathcal{O}(X \times_Y X)$ with $\mathcal{O}(X) \otimes_{\mathcal{O}(Y)} \mathcal{O}(X) = A \otimes_B A$ via the map

$$\theta(a \otimes a')(x,y) = a(x)a'(y), \qquad \text{with } \pi(x) = \pi(y).$$

This last condition implies the well-definition of θ. With this, we have the following result.

THEOREM 1.25 ([BF12, PROPOSITION 4]). *Let X be a complex affine variety with a right action of an affine algebraic group G and put $Y = X/G$. Let $A := \mathcal{O}(X)$, $B := \mathcal{O}(Y)$ and $H := \mathcal{O}(G)$ be the corresponding coordinate rings. Then the following assertions are equivalent:*

(i) *The action of G on X is free,*

(ii) *The map $\alpha^* : \mathcal{O}(X \times_Y X) \to \mathcal{O}(X \times G)$ given by $f \mapsto f \circ \alpha$ is bijective, where $\alpha : X \times G \to X \times_Y X$ is defined as $(x,g) \mapsto (x, xg)$.*

(iii) *The map $\beta : A \otimes_B A \to A \otimes H$ given by $\beta(a \otimes a') = a\rho(a')$ is bijective and thus $B \subset A$ is a right H-Galois extension.*

Basically, this theorem states that, in bundles, the freeness condition is equivalent to the Galois map being bijective. Hence, the Hopf Galois extension condition is a necessary condition to ensure a bundle is principal.

However, not all information about the topological spaces involved is encoded in their coordinate rings, so to make a transparent reflection of the richness of principal bundles, we require an additional condition.

DEFINITION 1.35 (PRINCIPAL COMODULE ALGEBRA, [BF12, DEFINITION 9]). Let H be a K-Hopf algebra with bijective antipode and let A be a right H-comodule algebra with structure map $\rho : A \to A \otimes H$. We say that A is a *principal H-comodule algebra*, if it satisfies the following conditions:

(PCA1) $A^{coH} \subset A$ is a right H-Galois extension.

(PCA2) (*Equivariant projectivity condition*) The map $B \otimes A \to A$, given by $b \otimes a \to ba$, splits as a left A^{coH}-module and right H-comodule morphisms.

As remarked in [BH09], the key idea here is that the concept of equivariant projectivity replaces that of faithful flatness used in general Hopf Galois theory. Under the hypothesis of bijective antipode, in a Hopf Galois extension these two concepts are equivalent, while in general only the implication "equivariant projectivity" ⇒ "faithful flatness" holds (cf. [SS05]).

The next result is due to [DGH01] and [BH04].

THEOREM 1.26 ([BF12, PROPOSITION 5]). *Let H be a $\mathbb{C}$-Hopf algebra with bijective antipode and let A be a right H-comodule algebra with structure map $\rho : A \to A \otimes H$. A is a principal H-comodule algebra if and only if it admits a strong connection form, that is, if there exists a map $\omega : H \to A \otimes A$, such that*

$$\omega(1) = 1 \otimes 1,$$
$$m_H\omega = u_H\varepsilon_H,$$
$$(\omega \otimes \mathrm{id}_H)\Delta = (\mathrm{id}_A \otimes \rho)\omega,$$
$$(S \otimes \omega)\Delta = (\tau_{A,H} \otimes \mathrm{id}_A)(\rho \otimes \mathrm{id}_A)\omega.$$

This theorem provides an effective method to verify the principality of a comodule algebra. For example, every cleft comodule algebra (cf. Definition 1.38) is a principal comodule algebra (cf. [BF12, Example 3]).

1.3.1.10 OTHER EXAMPLES

Several other examples of Hopf Galois extensions (HGE) are treated in the literature. The most remarkable are the following:

- Differential Galois theory, [Mon09, Example 2.13]: Let $E \supset \Bbbk$ be a field of characteristic $p > 0$ and let $\mathfrak{g} \subset \mathrm{Der}_{\Bbbk}(E)$ be a restricted Lie algebra of $\Bbbk$-derivations of E, which is finite-dimensional over $\Bbbk$. If the restricted enveloping algebra is denoted $u(\mathfrak{g})$ and it acts on E via $\mathfrak{g}$ acting as derivations, then for $H = u(\mathfrak{g})^*$, $E^{coH} = E^{\mathfrak{g}} = \{a \in E : x \cdot a = 0, \text{for all } x \in \mathfrak{g}\}$. $E^{\mathfrak{g}} \subset E$ is $u(\mathfrak{g})^*$-Galois if and only if $E \otimes_{\Bbbk} \mathfrak{g} \to \mathrm{Der}_{\Bbbk}(E)$ is injective.

- HGE for Azumaya algebras, [DT89, Theorem 6.20]: For a fixed Hopf algebra H, let E be an Azumaya algebra and let $C \subset E$ be a subalgebra such that the right C-module E is a progenerator. There is a 1-1 correspondence between the right H-Galois extensions $B^{coH} \subset B$ (such that there exists an algebra morphism $B \to E$ and $B^{coH} \cong C$) and the measuring actions of the form $E^C \otimes H \to E^C$, where $E^C := \{x \in E : cx = xc, \text{ for all } c \in C\}$.

- HGE for Calabi-Yau Hopf algebras, [Yu16]: In his paper, Yu showed that Hopf Galois objects of a twisted Calabi-Yau Hopf algebra with bijective antipode are still twisted Calabi-Yau, and gave their Nakayama automorphism explicitly. As applications, cleft objects (cf. Definition 1.38) of twisted Calabi-Yau Hopf algebras and Hopf Galois objects of the quantum automorphism groups of non-degenerate bilinear forms are proved to be twisted Calabi-Yau.

- HGE for monoidal Hom-Hopf algebras, [CZ16]: Analogous to the preliminaries for Hopf algebra theory presented in Section 1.1, the concept of Hom-Hopf algebra can be reviewed; Hom-type algebras appear in some physical contexts. In their paper, Chen and Zhang prove the Schneider's affineness theorem (cf. [Mon93, Theorem 8.5.6]) in the case of monoidal Hom-Hopf algebras in terms of total integrals and Hom-Hopf Galois extensions.

- HGE for pointed Hopf Hops algebras, [Gün99]: In his paper, Günther develops a systematic method to calculate cleft extensions for pointed Hopf algebras. In particular, cleft extensions for the quantum enveloping algebra $U_q(\mathfrak{sl}_2(\Bbbk))$ (cf. Example 1.11) and the Frobenius-Lusztig kernel $U_q(\mathfrak{sl}_2(\Bbbk))'$ were classified.

- HGE for Taft Hopf algebras, [Mas94]: In the paper of Masoka, cleft extensions for certain Hopf algebras generated by skew primitive elements are classified; a particular case is the Taft Hopf algebra of Example 1.10.

- HGE for the Drinfel'd double of the Taft algebra, [Sch99]: In general, the Drinfel'd double of a finite dimensional $\Bbbk$-Hopf algebra H is the tensor product algebra $D(H) = H \otimes H^*$. This construction is a quasi-triangular Hopf algebra. Roughly speaking, the Drinfel'd double of the Taft algebra can be seen as $U_q(\mathfrak{sl}_2(\Bbbk))'$ with two copies of the group-like generators. Schauenburg classifies all the Galois objects over $U_q(\mathfrak{sl}_2(\Bbbk))'$ and $D(T_{n^2}(\omega))$.

- Quantum principal bundles with a compact structure group, [Dur95]: Another generalization of classical principal bundles are the *quantum principal bundles* defined in [Dur94, Definition 3.1] with the help of $*$-algebras. In his paper, Đurđević shows that every quantum principal bundle with a compact structure group is a HGE.

- Reduced enveloping algebras, [Skr04, §6]: Let $\Bbbk$ be a field of characteristic $p > 0$, and let $\mathfrak{g}$ be a finite dimensional p-Lie algebra over $\Bbbk$. For $\xi \in \mathfrak{g}^*$, denote by $U_\xi(\mathfrak{g})$ the corresponding reduced enveloping algebra of $\mathfrak{g}$. In other words $U_\xi(\mathfrak{g})$ is the factor algebra of the universal

enveloping algebra $U(\mathfrak{g})$ by its ideal generated by central elements $x^p - x^{[p]} - \xi(x)^p 1$, with $x \in \mathfrak{g}$. Skryabin shows that $U_\xi(\mathfrak{g})$ is a $U_0(\mathfrak{g})^*$-Galois extension if and only if $U_\xi(\mathfrak{g})$ is central simple.

- HGE of structured ring spectra, [Rog08].
- Hopf Galois structures on Galois S_n-extension, [Tsa18].
- Hopf Galois structures of Heisenberg Type, [Kay19].

1.3.2 PROPERTIES

Since their first appearance, Hopf Galois extensions have been vividly studied and therefore used as a tool in the investigation and classification of Hopf algebras themselves. In this section we review some of their properties.

PROPOSITION 1.27 ([SCH90B, REMARK 1.1]). *Let $A^{coH} \subset A$ be a right H-Galois extension. Then*

(i) *$A \otimes_{A^{coH}} A$ is a Hopf module in ${}_A\mathrm{Mod}^H$ with left A-module structure via*

$$a(x \otimes y) = ax \otimes y, \qquad \text{for all } a, x, y \in A,$$

and right H-comodule structure via

$$x \otimes y \mapsto \sum x_0 \otimes y \otimes x_1, \qquad \text{for all } x, y \in A. \tag{1.37}$$

(ii) *$A \otimes H$ is a Hopf module in ${}_A\mathrm{Mod}^H$ with left A-module structure via*

$$a(x \otimes h) = ax \otimes h, \qquad \text{for all } a, x \in A \text{ and } h \in H,$$

and right H-comodule structure via

$$x \otimes h \mapsto \sum x_0 \otimes h_2 \otimes x_1 S(h_1), \qquad \text{for all } x \in A \text{ and } h \in H. \tag{1.38}$$

(iii) *$A \otimes_{A^{coH}} A$ is a Hopf module in Mod^H_A with right A-module structure via*

$$(x \otimes y)a = x \otimes ya, \qquad \text{for all } a, x, y \in A,$$

and right H-comodule structure via

$$x \otimes y \mapsto \sum x \otimes y_0 \otimes y_1, \qquad \text{for all } x, y \in A. \tag{1.39}$$

(iv) *$A \otimes H$ is a Hopf module in Mod^H_A with right A-module structure via*

$$(x \otimes h)a = \sum xa_0 \otimes ha_1, \qquad \text{for all } a, x \in A \text{ and } h \in H,$$

and right H-comodule structure via

$$x \otimes h \mapsto \sum x \otimes h_1 \otimes h_2, \qquad \text{for all } x \in A \text{ and } h \in H. \tag{1.40}$$

Hence, the Galois map $\beta : A \otimes_{A^{coH}} A \to A \otimes H$ is a morphism of Hopf modules, both in ${}_A\mathrm{Mod}^H$ and Mod^H_A.

The proof is a verification of the required compatibility (cf. Definition 1.27).

A classical theorem in Galois theory says that, if $F \subset E$ is a finite Galois extension of fields with Galois group G, then there exists $a \in E$ such that $\{x \cdot a : x \in G\}$ is basis for E over F. Such feature is known as the *normal basis property*. An important question in Hopf Galois theory is whether such property is satisfied.

DEFINITION 1.36 (RIGHT NORMAL BASIS PROPERTY, [MON93, DEFINITION 8.2.1]). Let A be a right H-comodule algebra and consider the algebra extension $A^{coH} \subset A$ (not necessarily being Galois). We say that the extension has the *right normal basis property*, if $A \cong A^{coH} \otimes H$ as left A^{coH}-modules and right H-comodules.

We review some basic facts about finite-dimensional Hopf algebras in order to show that, in this case, the normal basis property is equivalent to the classical notion.

DEFINITION 1.37 (INTEGRALS, [MON93, DEFINITION 2.1.1]). Let H be a K-Hopf algebra.

(i) A *left integral* in H is an element $\lambda \in H$ such that $h\lambda = \varepsilon(h)\lambda$, for all $h \in H$.

(ii) A *right integral* in H is an element $\lambda' \in H$ such that $\lambda' h = \varepsilon(h)\lambda'$, for all $h \in H$.

We denote the space of left (resp. right) integral by $\int^l_H$ (resp. $\int^r_H$).

If H is such that $\int^l_H = \int^r_H$, it is called *unimodular*. Examples of such situation can be found in [Mon93, Examples 2.1.2].

Using the Fundamental Theorem of Hopf modules, Larson and Sweedler proved that, if H is $\Bbbk$-finite-dimensional, both $\int^l_H$ and $\int^r_H$ are 1-dimensional (cf. [Mon93, Theorem 2.1.3]). Moreover, if $\lambda \in \int^l_H$ and $\lambda \neq 0$, H is a cyclic left H^*-module with generator λ for the action $\rightharpoonup$ described in Example 1.18. That is, we can identify H with $H^* \rightharpoonup \lambda$. Another result is that H is semisimple if and only if $\varepsilon(\int^l_H) \neq 0$ if and only if $\varepsilon(\in^r_H) \neq 0$. In this case, also $\int^l_H = \int^r_H$ and we may choose λ such that $\varepsilon(\lambda) = 1$ (cf. [Mon93, Theorem 2.2.1]).

PROPOSITION 1.28 ([MON09, LEMMA 3.5]). *Let H be a finite-dimensional $\Bbbk$-Hopf algebra such that $\dim_{\Bbbk}(H) = n$ and let A be a right H-comodule algebra. Consider H^* acting on A with $A^{H^*} = A^{coH}$. Then the following assertions are equivalent:*

(i) *There exists $u \in A$ and $\{f_i\} \subset H^*$ such that $\{f_1 \cdot u, \ldots, f_n \cdot u\}$ is a basis for the free left A^{coH}-module A (i.e., A has a normal basis over A^{coH} in the classical sense).*

(ii) *The algebra extension $A^{coH} \subset A$ has the right normal basis property.*

Proof. (i)⇒(ii): Assume that A has a normal basis over A^{coH} in the classical sense. Using the identification $H = H^* \rightharpoonup \lambda$ of the previous paragraph, we may consider the left H^*-module map $\phi : A^{coH} \otimes H \to A$ given by

$$\phi(b \otimes (f \rightharpoonup \lambda)) := b(f \cdot u), \qquad \text{for all } b \in A^{coH} \text{ and } f \in H^*.$$

$A^{coH} \otimes H$ is a left H^* module via $f \cdot (b \otimes h) = b \otimes (f \rightharpoonup h)$, since this is the dual of the right comodule structure given by $\mathrm{id} \otimes \Delta$. Thus, ϕ is a right H-comodule map. Since it is a left A^{coH}-module isomorphism, A^{coH} has the normal basis property.

(ii)⇒(i): Now, assume that there exists an isomorphism $\phi : A^{coH} \otimes H \to A$ of left A^{coH}-modules and right H-comodules. Given a $\Bbbk$-basis $\{f_1, \ldots, f_n\}$ for H^*, the set

$$\{1 \otimes (f_1 \rightharpoonup \lambda), \ldots, 1 \otimes (f_n \rightharpoonup \lambda)\}$$

is an A^{coH}-basis for $A^{coH} \otimes H$. Hence, it follows that $\{f_1 \cdot u, \ldots, f_n \cdot u\}$ is an A^{coH}-basis for A, where $u = \phi(1 \otimes \lambda)$. Thus $A^{coH} \subset A$ has a normal basis in the usual sense. □

In general, not all Hopf Galois extensions have the normal basis property (cf. [Mon93, Example 8.2.3]). However, a result of Doi and Takeuchi characterizes extensions having the normal basis property.

DEFINITION 1.38 (CLEFT EXTENSION, [MON93, DEFINITION 7.2.1]). Let A be a right H-comodule algebra. The algebra extension $A^{coH} \subset A$ is said to be *H-cleft* if there exists a right H-comodule map $\gamma : H \to B$ which is convolution invertible.

REMARK 14. If $A^{coH} \subset A$ is a H-cleft extension, then the map γ can always be chosen *normalized*, in the sense that $\gamma(1) = 1$. Indeed, if it is not normalized we can replace γ by $\gamma' = \gamma^{-1}(1)\gamma$; this is possible since 1 is a group-like element and hence $\gamma(1)$ is invertible with inverse $(\gamma(1))^{-1} = \gamma^{-1}(1)$.

THEOREM 1.29 ([DNR01, THEOREM 6.4.12]). *Let A be a right H-comodule algebra. Then the following assertions are equivalent:*

(i) *There exists an invertible 2-cocycle and an action of H on A^{coH} such that $A \cong A^{coH} \#_\sigma H$.*

(ii) *The extension $A^{coH} \subset A$ is H-cleft.*

(iii) *$A^{coH} \subset A$ is a H-Galois extension and has the normal basis property.*

Roughly speaking, this result establishes that every Hopf crossed product is "cleft" using the convolution invertible map $\gamma : H \to A$ given by $\gamma(h) = 1\#h$. The proof is extensive and can be found in [DNR01].

Now, we discuss some conditions equivalent to $A^H \subset H$ being H^*-Galois.

LEMMA 1.30 ([MON93, LEMMA 8.3.2]). *Let H be an arbitrary Hopf algebra and A a left H-module algebra. Then the following assertions hold:*

(i) *A is a left $A\#H$-module, via $(a\#h) \cdot b := a(h \cdot b)$, for all $a, b \in A$ and $h \in H$.*

(ii) *A is a right A^H-module, via right multiplication.*

(iii) *A is a $A\#H$-A^H-bimodule.*

(iv) *$A^H \cong \mathrm{End}({}_{A\#H}A)^{op}$ as algebras.*

Proof. (i) and (ii) are straightforward.

(iii) Let $a \in A^H$, $b\#h \in A\#H$ and $c \in A$. Hence, using the associativity of A we have

$$\begin{aligned}(b\#h)\cdot(ca) = b(h\cdot(ca)) &\overset{(1.19)}{=} b\left[\sum(h_1\cdot c)(h_2\cdot a)\right] = b\left[\sum(h_1\cdot c)\varepsilon(h_2)a\right]\\ &= b[(h\cdot c)a] = [b(h\cdot c)]a = [(b\#h)\cdot c]a.\end{aligned}$$

(iv) Let $\psi : A^H \to \mathrm{End}({}_{A\#H}A)$ be given by $a \mapsto a_r$, where a_r is the right multiplication by a in A^H. Notice that a_r is indeed a $A\#H$-map since, for all $a \in A^H$, $b\#h \in A\#H$ and $c \in A$, we have

$$a_r((b\#h)\cdot c) = [(b\#h)\cdot c]a = (b\#h)\cdot(ca) = (b\#h)\cdot a_r(c).$$

On the other hand, if $a, b \in A^H$ and $x \in {}_{A\#H}A$, then

$$\begin{aligned}\psi(a+b)(x) &= (a+b)_r(x) = x(a+b) = xa + xb = a_r(x) + b_r(x) = \psi(a)(x) + \psi(b)(x),\\ \psi(ab)(x) &= (ab)_r(x) = x(ab) = (xa)b = (a_r(x))b = b_r(a_r(x)) = b_r a_r(x),\\ \psi(1_A)(x) &= (1_A)_r(x) = x1_A = x = \mathrm{id}_A(x).\end{aligned}$$

Hence, ψ is an algebra anti-morphism. Clearly $a_r = 0$ if and only if $a1 = a = 0$, so ψ is injective. Moreover, it is surjective since for any $\sigma \in \mathrm{End}({}_{A\#H}A)$ and $a \in A$, we have

$$\sigma(a) = \sigma(a1_A) = \sigma(a(1_H\cdot 1_A)) = \sigma((a\#1_H)\cdot 1_A) = (a\#1_H)\cdot\sigma(1_A) = a(1_H\cdot\sigma(1_A)) = a\sigma(1_A),$$

and hence $\sigma = \sigma(1_A)_r = \psi(\sigma(1_A))$. Notice that $\sigma(1_A)$ is indeed an element of A^H since, for any $h \in H$,

$$h\cdot\sigma(1_A) = (1_A\#h)\cdot\sigma(1_A) = \sigma((1_A\#h)\cdot 1) = \sigma(h\cdot 1_A) \overset{(1.19)}{=} \varepsilon(h)\sigma(1_A). \qquad \square$$

When the antipode is bijective, the laterality in this result can be interchanged.

LEMMA 1.31 ([CFM90, LEMMA 0.3]). *Let H be an arbitrary Hopf algebra such that the antipode S is bijective, and let A be a left H-module algebra. Then the following assertions hold:*

(i) *A is a right $A\#H$-module, via*

$$b\cdot(a\#h) = S^{-1}(h)\cdot(ba), \qquad \text{for all } a, b \in A \text{ and } h \in H,$$

(ii) *$A^H \cong \mathrm{End}(A_{A\#H})$ as algebras.*

Proof. (i) The proof is similar to the one given for Lemma 1.30.

(ii) Let $\psi : A^H \to \mathrm{End}(A_{A\#H})$ be given by $a \mapsto a_l$, where a_l is the left multiplication by a in A^H. Notice that a_l is indeed an $A\#H$-map since, for all $a \in A^H$, $b \in A$ and $c\#h \in A\#H$, we have

$$a_l(b\cdot(c\#h)) = a_l(S^{-1}(h)\cdot(bc)) = a(S^{-1}(h)\cdot(bc)) = S^{-1}(h)\cdot(abc) = (ab)\cdot(c\#h) = a_l(b)\cdot(c\#h).$$

Here we used that the multiplication of A is a H-module map. On the other hand, if $a, b \in A^H$

and $x \in A_{A\#H}$, then

$$\begin{aligned}\psi(a+b)(x) &= (a+b)_l r(x) = (a+b)x = ax+bx = a_l(x)+b_l(x) = \psi(a)(x)+\psi(b)(x),\\ \psi(ab)(x) &= (ab)_l(x) = (ab)x = a(bx) = a(b_l(x)) = a_l(b_l(x)) = a_l b_l(x),\\ \psi(1_A)(x) &= (1_A)_l(x) = 1_A x = x = \mathrm{id}_A(x).\end{aligned}$$

Hence, ψ is an algebra morphism. Clearly $a_l = 0$ if and only if $1a = a = 0$, so ψ is injective. Moreover, it is surjective since for any $\sigma \in \mathrm{End}(A_{A\#H})$ and $a \in A$, we have

$$\begin{aligned}\sigma(a) &= \sigma(1_H \cdot a) = \sigma(S^{-1}(1_H)\cdot(1_A a)) = \sigma(1_A \cdot (a\#1_H)) = \sigma(1_A)\cdot(a\#1_H)\\ &= S^{-1}(1_H)\cdot(\sigma(1_A)a) = \sigma(1_A)a\end{aligned}$$

and hence $\sigma = \sigma(1_A)_l = \psi(\sigma(1_A))$. Notice that $\sigma(1_A)$ is indeed an element of A^H since, for any $h \in H$,

$$h\cdot\sigma(1_A) = \sigma(1_A)\cdot(1_A\#S(h)) = \sigma(1_A\cdot(1_A\#S(h))) = \sigma(h\cdot 1_A) \overset{(1.19)}{=} \varepsilon(h)\sigma(1). \qquad \square$$

Using Lemma 1.30 and the notion of *left trace function* (that is, maps of the form $\hat{\lambda} : A \to A^H$ such that $\hat{\lambda}(a) = \lambda a$, for some left integral $\lambda \neq 0$ in H), works of Doi, Kreimer, Takeuchi and Ulbrich lead to the following characterization of H^*-Galois extensions (cf. [DT86, KT81, vU82]).

THEOREM 1.32 ([MON93, THEOREM 8.3.3]). *Let H be a finite-dimensional $\Bbbk$-Hopf algebra and A a left H-module algebra (and thus, a right H^*-comodule). Then the following assertions are equivalent:*

(i) *$A^H \subset A$ is a right H^*-Galois extension.*

(ii) *The map $\pi : A\#H \to \mathrm{End}(A_{A^H})$ is an algebra morphism and A is finitely generated projective as right A^H-module.*

(iii) *A is a generator for the category of left $A\#H$-modules.*

(iv) *If $0 \neq \lambda \in \int_H^l$, then the map $[-,-] : A \otimes_{A^H} A \to A\#H$, given by $[a,b] = a\lambda b$, is surjective.*

(v) *For any left $A\#H$-module M, consider $A \otimes_{A^H} M^H$ as a left $A\#H$-module by letting $A\#H$ act on A via π. Then the map $\Phi : A \otimes_{A^H} M^H \to M$, given by $a \otimes m \mapsto a\cdot m$, is a left $A\#H$-module isomorphism.*

In [Mon09, Example 4.6] it is shown that, even for group actions, Theorem 1.32 does not necessarily holds.

Following [MR01, 1.1.6], for any two rings R and S, we say that they are *connected by a Morita context* if there exist a R-S-bimodule ${}_R V_S$, a S-R-bimodule ${}_S W_R$ and bimodule morphisms

$$[-,-] : W \otimes_R V \to S \qquad \text{and} \qquad (-,-) : V \otimes_S W \to R$$

such that, for all $v, v' \in V$ and $w, w' \in W$, the relations

$$v' \cdot [w,v] = (v',w)\cdot v \in V \qquad \text{and} \qquad [w,v]\cdot w' = w\cdot(v,w') \in W$$

hold. This is equivalent to saying that the array

$$T = \begin{bmatrix} R & V \\ W & S \end{bmatrix}$$

becomes an associative ring, where the formal operations are those of 2×2 matrices, using $[-,-]$ and $(-,-)$ to compute the multiplication.

When the two maps $[-,-]$ and $(-,-)$ are surjective, we say that the rings R and S are *Morita equivalent*. Notice that this is equivalent to saying that the four functors

$$\begin{aligned} -\otimes_R V &: \mathrm{Mod}_R \to \mathrm{Mod}_S, & -\otimes_S W &: \mathrm{Mod}_S \to \mathrm{Mod}_R \\ W\otimes_R - &: {}_R\mathrm{Mod} \to {}_S\mathrm{Mod} & V\otimes_S - &: {}_S\mathrm{Mod} \to {}_R\mathrm{Mod} \end{aligned}$$

are equivalences of categories (cf. [MR01, 3.5.5]).

We shall see that, for any finite-dimensional Hopf algebra H and any left H-module algebra A, such a set-up exists for the rings $R = A^H$ and $S = A\#H$, using $V = W = A$. By Lemma 1.30, we already guarantee that A is a $A\#H$-A^H-bimodule; however, the structure described in Lemma 1.31 is not enough for the other laterality to work. Hence, we proceed as follows: Recall that, if H is finite-dimensional, then S is bijective, and both $\int_H^r$ and $\int_H^l$ are one-dimensional (cf. [Mon93, Theorem 2.1.3]). Also notice that, if $0 \neq \lambda \in \int_H^l$, then $\lambda h \in \int_H^l$, for any $h \in H$. Thus, there exist $\alpha \in H^*$ such that

$$\lambda h = \alpha(h)\lambda \qquad \text{for all } h \in H.$$

With the notation of Example 1.18, we define $h^\alpha := \alpha \rightharpoonup h$. Since α is multiplicative, it is a group-like element of H^* and thus the map $h \mapsto h^\alpha$ is an automorphism of H. By [Rad76], $\lambda^\alpha = S(\alpha)$. We define our new right action of $A\#H$ on A by

$$a \cdot (b\#h) = S^{-1}h^\alpha \cdot (ab), \qquad \text{for all } a, b \in A \text{ and } h \in H. \tag{1.41}$$

Notice that this is the action of Lemma 1.31 but "twisted" by α.

THEOREM 1.33 ([CFM90, THEOREM 2.10]). *Let H be a finite-dimensional Hopf algebra and A a left H-module algebra (and hence, a right H^*-comodule algebra). Consider A in ${}_{A\#H}\mathrm{Mod}_{A^H}$ as in Lemma 1.30, and in ${}_{A^H}\mathrm{Mod}_{A\#H}$ with the right action of $A\#H$ given by (1.41). Then $V = {}_{A^H}A_{A\#H}$ and $W = {}_{A\#H}A_{A^H}$, together with the maps*

$$\begin{aligned} [-,-] &: A \otimes_{A^H} A \to A\#H & &\text{given by } [a,b] := a\lambda b, \\ (-,-) &: A \otimes_{A\#H} A \to A^H & &\text{given by } (a,b) := \lambda \cdot (ab), \end{aligned}$$

give a Morita context for A^H and $A\#H$.

Using the left trace function, $\hat{\lambda}(A) = \lambda \cdot A = (A,A)$. If we also consider the ideal $A\lambda A = [A,A]$, the next result is immediate.

COROLLARY 1.34 ([MON09, COROLLARY 4.9]). *Let H be a finite-dimensional Hopf algebra and A a left H-module algebra. If $0 \neq \lambda \in \int_H^l$ is such that the left trace function $\hat{\lambda} : A \to A^H$ is surjective and $A\lambda A = A\#H$, then $A\#H$ is Morita equivalent to A^H.*

Since simplicity of $A\#H$ implies that $A\lambda A = A\#H$ and semisimplicity of H implies that the trace function is surjective (cf. [CFM90, Corollary 1.3]), the next result follows from Theorem 1.32.

COROLLARY 1.35 ([MON09, COROLLARY 4.9]). *Let H be a semisimple finite-dimensional Hopf algebra and A a left H-module algebra such that $A\#H$ is a simple algebra. Then $A^H \subset A$ is H^*-Galois and A^H is Morita equivalent to $A\#H$.*

Finally, we mention a relevant result also involving equivalences of categories of modules.

THEOREM 1.36 ([SCH90A, THEOREM I]). *Let H be an arbitrary Hopf algebra with bijective antipode and A a right H-comodule algebra. Then the following assertions are equivalent:*

(i) *$A^{coH} \subset A$ is right H-Galois and A is a faithfully flat left (or right) A^{coH}-module.*

(ii) *The Galois map $\beta : A \otimes_{A^{coH}} A \to A \otimes H$ is surjective and A is an injective H-comodule.*

(iii) *The functor $\Phi : \mathrm{Mod}_{A^{coH}} \to \mathrm{Mod}_A^H$ given by $M \mapsto M \otimes_{A^{coH}} A$ is an equivalence.*

(iv) *The functor $\Phi' : {}_{A^{coH}}\mathrm{Mod} \to {}_A\mathrm{Mod}^H$ given by $M \mapsto A \otimes_{A^{coH}} M$ is an equivalence.*

Although in this section we tried to cover several properties of Hopf Galois extensions (HGE), the list is large and it would be impossible to address them all. Nevertheless, we shall some remarkable recent advances in Hopf Galois theory; we tried to list them in chronological order.

- Representation theory of HGE: In [Sch90b] some questions of representation theory were addressed for HGE, such as induction and restriction of simple or indecomposable modules. In particular, generalizations were given of classical results on representations of groups and Lie algebras.
- Maschke theorems for HGE: Classically, Maschke Theorem states that, if G is a finite group and $\Bbbk$ a field whose characteristic does not divide the order of G, then the group algebra $\Bbbk G$ is semisimple. For a finitely generated projective Hopf algebra H and a H-Galois extension $A^{coH} \subset A$, [Doi90] proved an analogous of Maschke Theorem, stating that, if A^{coH} is semisimple artinian, then so is A.
- Hopf biGalois objects and Galois theory for HGE: A result in [vOZ94] proves that, if $\Bbbk \subset A$ are fields such that $\Bbbk \subset A$ is a L-H-biGalois extension, then there is a one-to-one correspondence between the Hopf ideal of L and the H-costable intermediate fields $F \subset A$. This correspondence theorem is a generalization of the classical Galois connection in field extension theory. On the other hand, [Sch96] proves that the existence of a L-H-biGalois object is equivalent to H and L being monoidally co-Morita $\Bbbk$-equivalent, i.e, their monoidal categories of comodules are equivalent as monoidal $\Bbbk$-linear categories. This leads to another Galois correspondence that is studied in [Sch98]. More recently, the existence of a Galois connection between subalgebras of an H-comodule algebra and generalized quotients of the Hopf algebra H was proven in [MS09].
- Hopf Galois coextensions: We studied above the relation between HGE and the normal basis property; however, there exists a coalgebra version of the normal basis property

involving the notion of crossed coproduct and cleft coextension, introduced by [DMR96]. This is further studied in [CWW03] addressing the notion of Hopf Galois coextension and twisting techniques. More recently, this theory was used in [Has12] to show that Hopf Galois coextensions of coalgebras are the sources of stable anti Yetter-Drinfeld modules.

- Hochschild cohomology on HGE: In [Şte95], for a H-Galois extension $A^{coH} \subset A$, spectral sequences are constructed and used to connect the Hochschild cohomologies and homologies of A and A^{coH}. This is further studied in [MŞ10].

- HGE with central invariants: A H-Galois extension $A^{coH} \subset A$ is said to have central invariants if $A^{coH} \subset Z(A)$. In [Rum98] these HGE were studied, addressing some geometric properties which are close to those of principal bundles and Frobenius manifolds.

- Prime ideals in HGE: Let H be a finite-dimensional Hopf algebra and $A^{coH} \subset A$ a H-Galois extension such that A is a faithfully flat as a left A^{coH}-module. In [MS99] a comparison between the prime ideals of A^{coH} and of A was made, studying in particular the classical Krull relations. Since Hopf crossed products are examples of faithfully flat Galois extensions, those results were applied to crossed products. They also show that if H is semisimple and semisolvable, then A is semiprime, provided A^{coH} is H-semiprime.

- Cyclic homology of HGE: For a Hopf algebra H, the category $\mathscr{CM}_m(H)$ of modular crossed module over H was introduced in [JŞ06]. If $M \in \mathscr{CM}_m(H)$ and L is a Hopf subalgebra, they computed the cyclic homology of $H \otimes_L M$ under certain restrictions for L and M; this in particular was used to calculate the cyclic homology of group algebras, quantum tori and almost symmetric algebras. This is further studied in [HR13].

- Algebraic K-theory of HGE: The concept of principal extensions (cf. Definition 1.35) was firstly introduced in [BH04]; along the applications given in this document, principal extensions also were used to construct an explicit formula for the Chern–Galois character (which is a homomorphism of Abelian groups that assigns the homology class of an even cyclic cycle to the isomorphism class of a finite-dimensional corepresentation). On the other hand, years later [AW10] showed that the Cartan map from K-theory to G-theory of HGE is a rational isomorphism, provided the subalgebra of coinvariants is regular, the base Hopf algebra is finite-dimensional and its Cartan map is injective in degree zero. This, in particular, covers the case of a crossed product of a regular ring with a finite group and was applied to the study of Iwasawa modules.

- Generalized HGE: For an extension $A^{coH} \subset A$ to be H-Galois is required the bijectivity of the Galois map $\beta : A \otimes_{A^{coH}} A \to A \otimes H$. Criteria under which surjectivity of β (which is usually much easier to verify) is sufficient were studied in [SS05]; they used such criteria to investigate the structure of A as an A^{coH}-module and a H-comodule. In particular, equivariant projectivity of extensions in several important cases was proven. Moreover, they reconstructed the theory when the Hopf algebra H is interchanged for a quotient coalgebra or an one-sided module of a Hopf algebra. In parallel, [Bö05] also recreated the theory when H is a Hopf algebroid.

- Homotopy theory of HGE: As we have remarked before, HGE can be viewed as the noncommutative analogues of principal fibre bundles where the role of the structural group is

played by a Hopf algebra. It is therefore natural to adapt the concept of homotopy to them; such construction was made in [KS05]. In their paper, they classify HGE up to homotopy equivalence and some homotopy invariants were studied. More generally, in [Hes09], a theory of homotopic HGE in a monoidal category (with compatible model category structure) was introduced; this generalizes the case of structured ring spectra.

- HGE in braided tensor categories: Braided Hopf algebras have attracted much attention in both mathematics and mathematical physics since they play an important role in the classification of finite-dimensional pointed Hopf algebras (cf. [AS02]); the immediate generalization of such setup is the concept of braided tensor categories (BTC). Hence, [ZZ03] generalized HGE to BTC, showing that if the category $\mathscr{C}$ is BTC and has (co)equalizers, $A = B\#_\sigma H$ is a crossed product algebra if and only if the extension $B \subset A$ is Galois, the canonical map $q : A \otimes A \to A \otimes_B A$ is split and A is isomorphic as left B-modules and right H-comodules to $B \otimes H$ in $\mathscr{C}$ (cf. Theorem 1.29).

- Morita (auto)equivalences of HGE: Let $A^{coH} \subset A$ and $B^{coH} \subset B$ be two H-Galois extensions. In [CCMT07] was investigate the category ${}_A\mathrm{Mod}_B^H$ of relative Hopf bimodules and therefore the Morita equivalences between A and B induced by them. More recently, in [CM10] were addressed H-Morita autoequivalences of HGE, introduced the concept of H-Picard group, and established an exact sequence linking the H-Picard group of the comodule algebra A and the Picard group of A^{coH}.

- Generic HGE: [Kas09] deals with associative algebras ${}^\alpha H$, called twisted algebras, obtained from a Hopf algebra H by twisting its product by a cocycle α. They coincides with the class of cleft objects; as we saw in the examples, classical Galois extensions and strongly graded algebras belong to this class. Continuing his work in [AK08], where they attached two "universal algebras" $U(H)^\alpha$ and $A(H)^\alpha$ to each twisted algebra ${}^\alpha H$, Kassel studies the second algebra, $A(H)^\alpha$, which is a "generic" version of ${}^\alpha H$. Then, he calculates the generic cocycle cohomologous to the original cocycle α, and considers the commutative algebra $B(H)^\alpha$ generated by the values of the generic cocycle and of its convolution inverse. He proves that $A(H)^\alpha$ is a cleft H-Galois extension of $B(H)^\alpha$, called a generic H-Galois extension. Some theory regarding versal deformation spaces is developed.

- Cohen-Macaulay invariant subalgebra of dense HGE: Let H be a finite-dimensional Hopf algebra and A a left H-module (and hence, a right H^*-comodule). The algebra extension $A^H \subset A$ is called a H^*-dense Galois extension if the cokernel of the Galois map $\beta : A \otimes_{A^H} A \to A \otimes H^*$ is finite-dimensional (no bijectivity required). Obviously the concept of Hopf dense Galois extension is a weaker version of that of HGE. When H is semisimple and A is left H-noetherian, [HZ17] proved that A^H will inherit the AS-Cohen-Macaulay property from A under some mild conditions, and A, when viewed as a right A^H-module, is a Cohen-Macaulay module.

- HGE for Hopf categories: The concept of $\Bbbk$-algebra is translated to category theory with the notion of $\Bbbk$-linear category; similarly, there exist categorical versions of bialgebras and Hopf algebras, respectively termed $\Bbbk$-linear semi-Hopf categories and $\Bbbk$-linear Hopf categories. It turns out that several classical properties of Hopf algebras can be generalized to Hopf categories (cf. [BCV16]). In [CF18] a notion of Hopf-Galois category extension

is introduced and studied. Later in this document we will mention descent datums; the cited paper also extended this notion to categories.

1.4 QUANTUM TORSORS

We saw in Example 1.3.1.9 that the notion of (classical) torsor is present in many algebraic formulations of different contexts, such as vector bundle, affine scheme, categorical bundles, etc.; furthermore, dualizing such setup, we motivated the notion of Hopf Galois extension based on the bijectivity of the map α^*. However, in recent years other approaches to non-commutative torsors have been achieved. In this section we review the one given by [Gru03] in which, instead of working with α^* and the freeness of the action, a "parallelogram" property of torsors is used.

Following [Bae09], we shall give a rough motivation to this "parallelogram" property with one simple example, although a more detailed can be found in [Gru03, §1.2] for torsors in general.

Recall that, when working with vectors on the euclidean plane, a point is fixed and called the *origin*. Thus, any point in the plane is identified with the arrow going from the origin to that point. This lets us add points in the plane by adding their arrows (in other words, the parallelogram property), making $\mathbb{R}^2$ a group. However, if we forget the origin, we lost the identification of points with arrows. In this case we can not longer add them, but we can still subtract two of them and get an arrow. Thus, the plane (without origin) is a $\mathbb{R}^2$-torsor. The moral of this is that, although we are not longer able to apply the parallelogram property with arrows, we can still associate to three points a, b, c a fourth point d such that a, b, c, d is a parallelogram. In multiplicative notation for an arbitrary G-torsor, we have identified the assignation $(a, b, c) \mapsto d := ab^{-1}c$.

The following axioms dualize this setup to the non-commutative case.

DEFINITION 1.39 (QUANTUM TORSOR, [SCH03, DEFINITION 3.1]). A *quantum K-torsor* is a K-algebra T together with an algebra morphism $\mu : T \to T \otimes T^{op} \otimes T$ such that the following diagrams commute:

$$\begin{array}{ccc} T & \xrightarrow{\mu} & T \otimes T^{op} \otimes T \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_T \otimes \mathrm{id}_{T^{op}} \otimes \mu} \\ T \otimes T^{op} \otimes T & \xrightarrow[\mu \otimes \mathrm{id}_{T^{op}} \otimes \mathrm{id}_T]{} & T \otimes T^{op} \otimes T \otimes T^{op} \otimes T \end{array} \qquad \begin{array}{ccccc} & & T & & \\ & {\scriptstyle \mathrm{id}_T \otimes u}\swarrow & \downarrow{\scriptstyle u} & \searrow{\scriptstyle u \otimes \mathrm{id}_T} & \\ T \otimes T & \xleftarrow[\mathrm{id}_T \otimes m]{} & T \otimes T \otimes T & \xrightarrow[m \otimes \mathrm{id}_T]{} & T \otimes T \end{array}$$

Following [Gru03], we extend Sweedler's sigma notation.

NOTATION (GENERALIZED SWEEDLER'S SIGMA NOTATION FOR QUANTUM TORSORS). Let T be a K-torsor with associated map $\mu : T \to T \otimes T^{op} \otimes T$. For all $x \in T$, forgetting the summation symbol, we denote

$$\mu(x) = x^{(1)} \otimes x^{(2)} \otimes x^{(3)}.$$

With this, the left diagram of Definition 1.39 can be written as

$$\mu(x^{(1)}) \otimes x^{(2)} \otimes x^{(3)} = x^{(1)} \otimes x^{(2)} \otimes \mu(x^{(3)}), \tag{1.42}$$

while right diagram states

$$x^{(1)} \otimes x^{(2)} x^{(3)} = x \otimes 1_T,$$
$$x^{(1)} x^{(2)} \otimes x^{(3)} = 1_T \otimes x.$$

The torsor is said to be *commutative* if T is a commutative algebra. If $\mu = \mu^{op}$, where $\mu^{op}(x) = x^{(3)} \otimes x^{(2)} \otimes x^{(1)}$, the torsor is said to be *equipped with a commutative law.*

In order to relate quantum torsors with Hopf Galois extensions, we briefly recall the mechanism of *faithfully flat descent* for extensions of non-commutative rings and a related result.

DEFINITION 1.40 (DESCENT DATUM, [SCH03, DEFINITION 2.1]). Let R be a subring of the ring S, with the inclusion map denoted by $\eta : R \to S$, and let M be a left S-module with structure map $\gamma : S \otimes M \to M$. An S/R*-descent datum on* M is a left S-module map $D : M \to S \otimes_R M$ such that the following diagrams commute:

$$\begin{array}{ccc} M & \xrightarrow{D} & S \otimes_R M \\ {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_S \otimes_R D} \\ S \otimes_R M & \xrightarrow[\mathrm{id}_S \otimes_R \eta \otimes_R \mathrm{id}_M]{} & S \otimes_R S \otimes_R M \end{array} \qquad \begin{array}{ccc} M & \xrightarrow{D} & S \otimes_R M \\ & {\scriptstyle \mathrm{id}_M} \searrow & \downarrow{\scriptstyle \gamma} \\ & & M \end{array} \tag{1.43}$$

Consider the pairs (M, D), consisting of a S-module M and a S/R-descent datum D on M, together with arrows $f : (M, D) \to (N, E)$, where $f : M \to N$ is a S-module morphism such that $Ef = (\mathrm{id}_S \otimes f)D$. This category is denoted by $\mathrm{DD}(S/R)$.

When S is faithfully flat as right R-module, there exists an equivalence between the category of left R-modules and the category describe above.

LEMMA 1.37 (BECK'S THEOREM, [SCH03, THEOREM 2.2]). *Let R be a subring of the ring S, with the inclusion map denoted by $\eta : R \to S$. If the category of left R-modules is denoted by ${}_R\mathrm{Mod}$, then the assignation ${}_R\mathrm{Mod} \to \mathrm{DD}(S/R)$ given by $N \mapsto (S \otimes_R N, D)$, where*

$$D(s \otimes n) = s \otimes 1 \otimes n \in S \otimes_R \otimes S \otimes_R N,$$

induces a functor. Moreover, if S is faithfully flat as right R-module, then this functor is an equivalence. The inverse equivalence is given in objects as

$$(M, D) \mapsto {}^D M := \{m \in M : D(m) = 1 \otimes m\}.$$

In particular, for every descent datum (M, D), the map $f : S \otimes_R {}^D M \to M$ given by $s \otimes m \mapsto sm$ is an isomorphism with inverse induced by D, i.e., $f^{-1} : M \to S \otimes_R {}^D M$ is given by $f^{-1}(m) = D(m)$.

The next result shows that every torsor induces a decent datum.

LEMMA 1.38 ([SCH03, LEMMA 3.3]). *Let T be a quantum K-torsor. If $\mu : T \to T \otimes T^{op} \otimes T$ is the associated map to T, then*

$$D := (m \otimes \mathrm{id}_T \otimes \mathrm{id}_T)(\mathrm{id}_T \otimes \mu) : T \otimes T \to T \otimes T \otimes T$$

is a T/K-decent datum on the left T-module $T\otimes T$. Moreover, it satisfies

$$(\mathrm{id}_T\otimes D)\mu(x) = x^{(1)}\otimes 1\otimes x^{(2)}\otimes x^{(3)} = (\mathrm{id}_T\otimes 1_T\otimes \mathrm{id}_T\otimes \mathrm{id}_T)\mu(x).$$

REMARK 15. For the sake of notation, we will denote an arbitrary element of $T\otimes T$ by $x\otimes y$, without necessarily implying that it is a simple tensor. We also drop the summation symbol in coalgebras and right comodules, simply writing $\Delta(c) = c_{(1)}\otimes c_{(2)}$ and $\rho(n) = n_{(0)}\otimes n_{(1)}$ for the respective operations.

Proof of Lemma 1.38. In Sweedler's sigma notation, for every $x\otimes y\in T\otimes T$, we have

$$D(x\otimes y) = xy^{(1)}\otimes y^{(2)}\otimes y^{(3)}.$$

Left T-linearity of this map is obvious. Additionally, for every $x\otimes y\in T\otimes T$ we have

$$\begin{aligned}
(\mathrm{id}_T\otimes D)D(x\otimes y) &= (\mathrm{id}_T\otimes D)(xy^{(1)}\otimes y^{(2)}\otimes y^{(3)}) = xy^{(1)}\otimes D(y^{(2)}\otimes y^{(3)})\\
&= xy^{(1)}\otimes (m\otimes \mathrm{id}_T\otimes \mathrm{id}_T)(y^{(2)}\otimes \mu(y^{(3)}))\\
&= (m\otimes m\otimes \mathrm{id}_T\otimes \mathrm{id}_T)(x\otimes y^{(1)}\otimes y^{(2)}\otimes \mu(y^{(3)}))\\
&= (m\otimes m\otimes \mathrm{id}_T\otimes \mathrm{id}_T)(x\otimes \mu(y^{(1)})\otimes y^{(2)}\otimes y^{(3)})\\
&= (m\otimes \mathrm{id}_T\otimes \mathrm{id}_T\otimes \mathrm{id}_T)(x\otimes y^{(1)\,(1)}\otimes y^{(1)\,(2)}y^{(1)\,(3)}\otimes y^{(2)}\otimes y^{(3)})\\
&= (m\otimes \mathrm{id}_T\otimes \mathrm{id}_T\otimes \mathrm{id}_T)(x\otimes y^{(1)}\otimes 1_T\otimes y^{(2)}\otimes y^{(3)})\\
&= xy^{(1)}\otimes 1_T\otimes y^{(2)}\otimes y^{(3)}\\
&= (\mathrm{id}_T\otimes 1_T\otimes \mathrm{id}_{T\otimes T})(xy^{(1)}\otimes y^{(2)}\otimes y^{(3)})\\
&= (\mathrm{id}_T\otimes 1_T\otimes \mathrm{id}_{T\otimes T})D(x\otimes y),
\end{aligned}$$

which confirms the commutativity of the left diagram in Definition 1.40. For the right diagram, we have

$$\begin{aligned}
\gamma_{T\otimes T}D(x\otimes y) &= \gamma_{T\otimes T}(xy^{(1)}\otimes y^{(2)}\otimes y^{(3)}) = xy^{(1)}y^{(2)}\otimes y^{(3)}\\
&= (m\otimes \mathrm{id}_T)(x\otimes y^{(1)}y^{(2)}\otimes y^{(3)}) = (m\otimes \mathrm{id}_T)(x\otimes 1_T\otimes y) = x\otimes y.
\end{aligned}$$

Hence, D is a T/K-decent datum on the left T-module $T\otimes T$. □

Now, we are ready to prove a remarkable result. It states that every faithfully flat quantum K-torsor T is a right H-Galois object, for a suitable Hopf algebra H provided by the categorical equivalence of Lemma 1.38.

THEOREM 1.39 ([SCH03, THEOREM 3.4]). *Let T be a faithfully flat quantum K-torsor and*

$$H := {}^D(T\otimes T) = \{x\otimes y\in T\otimes T : xy^{(1)}\otimes y^{(2)}\otimes y^{(3)} = 1\otimes x\otimes y\}.$$

Then the following assertions hold:

(i) *H is a Hopf algebra. The algebra structure is that of a subalgebra of $T^{op}\otimes T$; comultiplica-*

tion and counit are given by

$$\Delta(x\otimes y)=x\otimes y^{(1)}\otimes y^{(2)}\otimes y^{(3)} \qquad \textit{and} \qquad \varepsilon(x\otimes y)=xy.$$

(ii) *T is a right H-comodule algebra with structure map given by*

$$\rho(x)=\mu(x)=x^{(1)}\otimes x^{(2)}\otimes x^{(3)}.$$

Moreover, $T^{coH}=K$.

(iii) *T is a right H-Galois object.*

Proof. (i) Since μ is a morphism of algebras, given $x\otimes y, a\otimes b\in H$, we have

$$\begin{aligned} D[(x\otimes y)(a\otimes b)] &= D(xa\otimes yb)=xa(yb)^{(1)}\otimes(yb)^{(2)}\otimes(yb)^{(3)}=xay^{(1)}b^{(1)}\otimes b^{(2)}y^{(2)}\otimes y^{(3)}b^{(3)}\\ &= ab^{(1)}\otimes b^{(2)}x\otimes yb^{(3)}=1\otimes ax\otimes yb=1\otimes xa\otimes yb=1\otimes(x\otimes y)(a\otimes b). \end{aligned}$$

Here we used that the second coordinate of the tensor is in T^{op}. The above proves that H is a subalgebra of $T^{op}\otimes T$. Now, since H is faithfully flat, it is the equalizer of

$$T\otimes T\otimes H \underset{D\otimes \mathrm{id}_H}{\overset{u_T\otimes \mathrm{id}_T\otimes \mathrm{id}_T\otimes \mathrm{id}_H}{\rightrightarrows}} T\otimes T\otimes T\otimes H$$

and thus the image of Δ is contained in $H\otimes H$, showing that Δ is well defined. Now, if $x\otimes y\in H$, then

$$[(\mathrm{id}_H\otimes\Delta)\Delta](x\otimes y)=(\mathrm{id}_H\otimes\Delta)(x\otimes y^{(1)}\otimes y^{(2)}\otimes y^{(3)})=x\otimes y^{(1)}\otimes y^{(2)}\otimes(y^{(3)})^{(1)}\otimes(y^{(3)})^{(2)}\otimes(y^{(3)})^{(3)},$$

while

$$[(\Delta\otimes\mathrm{id}_H)\Delta](x\otimes y)=(\Delta\otimes\mathrm{id}_H)(x\otimes y^{(1)}\otimes y^{(2)}\otimes y^{(3)})=x\otimes(y^{(1)})^{(1)}\otimes(y^{(1)})^{(2)}\otimes(y^{(1)})^{(3)}\otimes y^{(2)}\otimes y^{(3)}.$$

By (1.42) these two expressions are equivalent, proving the coassociativity of Δ. Moreover, Δ is an algebra map since μ is. On the other hand, if $x\otimes y\in H$, we have $xy\otimes 1=xy^{(1)}\otimes y^{(2)}y^{(3)}=1\otimes xy$, whence $xy\in K$ by faithful flatness of T. This proves that ε is well defined. Moreover,

$$\begin{aligned} [(\varepsilon\otimes\mathrm{id}_H)\Delta](x\otimes y)&=(\varepsilon\otimes\mathrm{id}_H)(x\otimes y^{(1)}\otimes y^{(2)}\otimes y^{(3)})=xy^{(1)}\otimes y^{(2)}\otimes y^{(3)}=1\otimes x\otimes y,\\ [(\mathrm{id}_H\otimes\varepsilon)\Delta](x\otimes y)&=(\mathrm{id}_H\otimes\varepsilon)(x\otimes y^{(1)}\otimes y^{(2)}\otimes y^{(3)})=x\otimes y^{(1)}\otimes y^{(2)}y^{(3)}=x\otimes y\otimes 1. \end{aligned}$$

This proves the main property of the counit. Is easy to check that ε is an algebra morphism. Therefore H is a K-bialgebra. Once (ii)-(iii) are proven below, we can invoke Remark 10 to guarantee that H is in fact a Hopf algebra.

(ii) In order to prove that $\rho: T\to T\otimes H$ is well defined, we have to check that the image of μ

is contained in $T \otimes H$, which is, by faithful flatness of T, the equalizer of

$$T \otimes T \otimes T \underset{\mathrm{id}_T \otimes D}{\overset{\mathrm{id}_T \otimes u_T \otimes \mathrm{id}_T \otimes \mathrm{id}_T}{\rightrightarrows}} T \otimes T \otimes T \otimes T$$

But in the proof of Lemma 1.38 was shown that $(\mathrm{id}_T \otimes D) = (\mathrm{id}_T \otimes 1_T \otimes \mathrm{id}_T \otimes \mathrm{id}_T)$. On the other hand, since μ is an algebra morphism, so is ρ. Finally, using Proposition 1.8 we have that T is a right H-comodule. Moreover, if $x \in T^{coH}$ then $x \otimes 1 = x^{(1)}x^{(2)} \otimes x^{(3)} = 1 \otimes x \in T \otimes T$, whence $x \in K$ by faithful flatness of T; the other contenence is straightforward.

(iii) The Galois map $\beta : T \otimes T \to T \otimes H$ is given by

$$\beta(x \otimes y) = (x \otimes 1 \otimes 1)\rho(y) = xy^{(1)} \otimes y^{(2)} \otimes y^{(3)} = D(x \otimes y)$$

By Lemma 1.37, β is an isomorphism. It follows that H is faithfully flat over K. □

In [Gru03], as part of Definition 1.39, an algebra morphism $\theta : T \to T$ satisfying

$$(\mathrm{id}_T \otimes \mathrm{id}_{T^{op}} \otimes \theta \otimes \mathrm{id}_{T^{op}} \otimes \mathrm{id}_T)(\mu \otimes \mathrm{id}_{T^{op}} \otimes \mathrm{id}_T)\mu = (\mathrm{id}_T \otimes \mu^{op} \otimes \mathrm{id}_T)\mu, \tag{1.44}$$

$$(\theta \otimes \theta \otimes \theta)\mu = \mu\theta, \tag{1.45}$$

is also required. [Sch03] called θ a *Grunspan map*. However, as remarked in [Gru03, Note 2.3], θ is fully determined by the multiplication of T and μ, via

$$(m \otimes \mathrm{id}_T \otimes m)(\mathrm{id}_T \otimes \mu^{op} \otimes \mathrm{id}_T)\mu(x) = 1_T \otimes \theta(x) \otimes 1_T.$$

In Sweedler's sigma notation this can be stated as

$$\theta(x) = x^{(1)}x^{(2)\,(3)}x^{(2)\,(2)}x^{(2)\,(1)}x^{(3)}.$$

Notice that if T is either commutative or equipped with a commutative law, then $\theta = \mathrm{id}_T$. If θ is bijective, the quantum torsor is said to be *autonomous*.

As we shall see later, the existence of the Grunspan map is demonstrable, and hence it is not necessary to require it in Definition 1.39. For that, we prove some preliminaries in order to enunciate the converse of Theorem 1.39.

Let H be an arbitrary K-Hopf algebra and T a right H-Galois object with bijective Galois map $\beta : T \otimes T \to T \otimes H$. We define $\gamma : H \to T \otimes T$ by

$$\gamma(h) := \beta^{-1}(1 \otimes h), \qquad \text{for all } h \in H, \tag{1.46}$$

and write $\gamma(h) = h^{[1]} \otimes h^{[2]} \in T \otimes T$. Notice that $h^{[1]} \otimes h^{[2]}$ is not necessary a simple tensor. With this notation, we obtain the following formulas.

LEMMA 1.40 ([SCH90B, REMARK 3.4]). *Let H be an arbitrary K-Hopf algebra and T a H-Galois*

object. Then $\gamma : H \to T \otimes T$ *defined by* (1.46) *satisfies the following relations:*

$$x_{(0)}{x_{(1)}}^{[1]} \otimes {x_{(1)}}^{[2]} = 1 \otimes x, \qquad \text{for all } x \in T, \tag{1.47}$$
$$h^{[1]}h^{[2]} = \varepsilon(h), \qquad \text{for all } h \in H, \tag{1.48}$$
$$h^{[1]}{h^{[2]}}_{(0)} \otimes {h^{[2]}}_{(1)} = 1 \otimes h, \qquad \text{for all } h \in H, \tag{1.49}$$
$${h^{[1]}}_{(0)} \otimes {h^{[2]}}_{(0)} \otimes {h^{[2]}}_{(1)} = {h_{(1)}}^{[1]} \otimes {h_{(1)}}^{[2]} \otimes h_{(2)}, \qquad \text{for all } h \in H, \tag{1.50}$$
$${h^{[1]}}_{(0)} \otimes {h^{[2]}}_{(0)} \otimes {h^{[1]}}_{(1)} = {h_{(2)}}^{[1]} \otimes {h_{(2)}}^{[2]} \otimes S(h_{(1)}), \qquad \text{for all } h \in H, \tag{1.51}$$
$$(gh)^{[1]} \otimes (gh)^{[2]} = h^{[1]}g^{[1]} \otimes g^{[2]}h^{[2]}, \qquad \text{for all } h, g \in H, \tag{1.52}$$
$$1^{[1]} \otimes 1^{[2]} = 1 \otimes 1. \tag{1.53}$$

Proof. Recall that, since T is a H-Galois object, there exist an structure map $\rho : T \to T \otimes H$ endowing T with a right H-comodule algebra structure. Hence, $\beta = (m_T \otimes \mathrm{id}_H)(\mathrm{id}_T \otimes \rho)$ is an algebra morphism. Then, for all $x \in T$ we have,

$$\begin{aligned}\beta(x_{(0)}{x_{(1)}}^{[1]} \otimes {x_{(1)}}^{[2]}) &= \beta(x_{(0)} \otimes 1)\beta(\gamma(x_{(1)})) = (x_{(0)} \otimes 1)\beta(\beta^{-1}(1 \otimes x_{(1)})) = (x_{(0)} \otimes 1)(1 \otimes x_{(1)}) \\ &= x_{(0)} \otimes x_{(1)} = 1x_{(0)} \otimes x_{(1)} = (1 \otimes 1)\rho(x) = \beta(1 \otimes x),\end{aligned}$$

an hence, applying β^{-1}, we get (1.47).

Now, since for every $x \otimes y \in T \otimes T$,

$$[(\mathrm{id}_T \otimes \varepsilon)\beta](x \otimes y) = (\mathrm{id}_T \otimes \varepsilon)(xy_0 \otimes y_1) = xy_0 \otimes \varepsilon(y_1) = xy_0\varepsilon(y_1) \otimes 1_H = xy \otimes 1_H.$$

We get $(\mathrm{id}_T \otimes \varepsilon)\beta = (m \otimes 1_H)$. Applying to β^{-1}, we get (1.48).

(1.49) immediately follows from

$$h^{[1]}{h^{[2]}}_{(0)} \otimes {h^{[2]}}_{(1)} = (h^{[1]} \otimes 1)\rho(h^{[2]}) = \beta(h^{[1]} \otimes h^{[2]}) = \beta(\beta^{-1})(1 \otimes h) = 1 \otimes h.$$

Now, if $\rho_{T\otimes T}$ (resp. $\rho_{T\otimes H}$) denotes the structure map of $T \otimes T$ (resp. $T \otimes H$) as right H-comodule via (1.39) (resp. (1.40)), the H-collinearity of β (cf. Proposition 1.27) guaranties

$$\rho_{T\otimes H}\beta = (\beta \otimes \mathrm{id}_H)\rho_{T\otimes T}.$$

Hence, for all $h \in H$ we have

$$\begin{aligned}(\beta \otimes \mathrm{id}_T)(h^{[1]} \otimes {h^{[2]}}_{(0)} \otimes {h^{[2]}}_{(1)}) &= [(\beta \otimes \mathrm{id}_H)\rho_{T\otimes T}](h^{[1]} \otimes h^{[2]}) = \rho_{T\otimes H}\beta(\gamma(h)) = \rho_{T\otimes H}(1 \otimes h) \\ &= 1 \otimes h_{(1)} \otimes h_{(2)} = \beta(\gamma(h_{(1)})) \otimes h_{(2)} = (\beta \otimes \mathrm{id}_T)({h_{(1)}}^{[1]} \otimes {h_{(1)}}^{[2]} \otimes h_{(2)}),\end{aligned}$$

which proves (1.50).

Similarly, (1.51) follows from the collinearity of β in the sense of (1.37) and (1.38). Finally, to prove (1.52) apply β and use (1.50). □

Notice that (1.52)-(1.53) say that $\gamma : H \to T^{op} \otimes T$ is an algebra morphism.

LEMMA 1.41 ([SCH02, LEMMA 3.1]). *Let* T *be a faithfully flat* H*-Galois object. Then*

$$S(x_{(1)})^{[1]} \otimes x_{(0)}S(x_{(1)})^{[2]} \in T \otimes K \subset T \otimes T, \qquad \text{for all } x \in T, \tag{1.54}$$

and

$$h^{[1]}_{(1)} \otimes S(h_{(2)})^{[1]} \otimes h^{[2]}_{(1)} S(h_{(2)})^{[2]} \in T \otimes T \otimes K \subset T \otimes T \otimes T, \qquad \textit{for all } h \in H. \tag{1.55}$$

Proof. If $\rho : T \to T \otimes H$ is the structure map of T as H-comodule algebra, for $x \in T$ we have

$$\begin{aligned} S(x_{(1)})^{[1]} \otimes \rho(x_{(0)} S(x_{(1)})^{[2]}) &= S(x_{(2)})^{[1]} \otimes x_{(0)} S(x_{(2)})^{[2]}{}_{(0)} \otimes x_{(1)} S(x_{(2)})^{[2]}{}_{(1)} \\ &\overset{(1.50)}{=} S(x_{(2)})_{(1)}{}^{[1]} \otimes x_{(0)} S(x_{(2)})_{(1)}{}^{[2]} \otimes x_{(1)} S(x_{(2)})_{(2)} \\ &= S(x_{(3)})^{[1]} \otimes x_{(0)} S(x_{(3)})^{[2]} \otimes x_{(1)} S(x_{(2)}) \\ &= S(x_{(1)})^{[1]} \otimes x_{(0)} S(x_{(1)})^{[2]} \otimes 1, \end{aligned}$$

in $T \otimes T \otimes H$. Since $T^{coH} = K$ and T is flat over K, this proves the first claim. Similarly, for $h \in H$ we have

$$\begin{aligned} h_{(1)}{}^{[1]} \otimes S(h_2)^{[1]} \otimes \rho(h_{(1)}{}^{[2]} S(h_{(2)})^{[2]}) &\overset{(1.50)}{=} h^{[1]}_{(1)} \otimes S(h_{(3)})_{(1)}{}^{[1]} \otimes h_{(1)}{}^{[2]} S(h_{(3)})_{(1)}{}^{[2]} \otimes h_{(2)} S(h_{(3)})_{(2)} \\ &= h_{(1)}{}^{[1]} \otimes S(h_{(4)})^{[1]} \otimes h_{(1)}{}^{[2]} S(h_{(4)})^{[2]} \otimes h_{(2)} S(h_{(3)}) \\ &= h_{(1)}{}^{[1]} \otimes S(h_{(2)})^{[1]} \otimes h_{(1)}{}^{[2]} S(h_{(2)})^{[2]} \otimes 1, \end{aligned}$$

proving the second claim, again by flatness of T. □

Roughly speaking, this result says that the elements $x_{(0)} S(x_{(1)})^{[2]}$ and $h_{(1)}{}^{[2]} S(h_{(2)})^{[2]}$ behave like scalars and hence, in calculation below, we will be able to move these around freely in any K-multilinear expression.

THEOREM 1.42 ([SCH02, THEOREM 3.2]). *Let T be a faithfully flat H-Galois object. Then T is a quantum K-torsor with associated map $\mu : T \to T \otimes T^{op} \otimes T$ defined by*

$$\mu(x) = (\mathrm{id}_T \otimes \gamma)\rho(x) = x_{(0)} \otimes x_{(1)}{}^{[1]} \otimes x_{(1)}{}^{[2]}, \qquad \textit{for all } x \in T.$$

Moreover, T has a Grunspan map $\theta : T \to T$ given by

$$\theta(x) = (x_{(0)} S(x_{(1)})^{[2]}) S(x_{(1)})^{[1]} = S(x_{(1)})^{[1]} (x_{(0)} S(x_{(1)})^{[2]}).$$

Proof. For all calculations, we let $x, y \in T$ and $h \in H$. Notice that, since ρ and γ are algebra morphisms, so is μ. We have,

$$\begin{aligned} (\mathrm{id}_T \otimes \mathrm{id}_{T^{op}} \otimes \mu)\mu(x) = (\mathrm{id}_T \otimes \mathrm{id}_{T^{op}} \otimes \mu)(x_{(0)} \otimes x_{(1)}{}^{[1]} \otimes x_{(1)}{}^{[2]}) &= x_{(0)} \otimes x_{(1)}{}^{[1]} \otimes \mu(x_{(1)}{}^{[2]}) \\ = x_{(0)} \otimes x_{(1)}{}^{[1]} \otimes x_{(1)}{}^{[2]} \otimes \gamma(x_{(1)}{}^{[2]}{}_{(1)}) &\overset{(1.50)}{=} x_{(0)} \otimes x_{(1)}{}^{[1]} \otimes x_{(1)}{}^{[2]} \otimes \gamma(x_{(2)}) \\ = \mu(x_{(0)}) \otimes \gamma(x_{(1)}) = (\mu \otimes \mathrm{id}_{T^{op}} \otimes_T)\mu(x), \end{aligned}$$

which proves the commutativity of the left diagram in (1.43). Additionally we have,

$$(\mathrm{id}_T \otimes m)\mu(x) = (\mathrm{id}_T \otimes m)(x_{(0)} \otimes x_{(1)}{}^{[1]} \otimes x_{(1)}{}^{[2]}) = x_{(0)} \otimes x_{(1)}{}^{[1]} x_{(1)}{}^{[2]} \overset{(1.48)}{=} x_{(0)} \otimes \varepsilon(x_{(1)}) = x \otimes 1.$$

On the other hand,

$$(m\otimes \mathrm{id}_T)\mu(x) = (m\otimes \mathrm{id}_T)(x_{(0)}\otimes {x_{(1)}}^{[1]}\otimes {x_{(1)}}^{[2]}) = x_{(0)}{x_{(1)}}^{[1]}\otimes {x_{(1)}}^{[2]} \overset{(1.47)}{=} 1\otimes x.$$

These two relations prove the commutativity of the right diagram in (1.43). Hence, T is a quantum K-torsor.
Now, since

$$\begin{aligned}\theta(xy) &= ((xy)_{(0)}S((xy)_{(1)})^{[2]})S((xy)_{(1)})^{[1]} = x_{(0)}y_{(0)}S(x_{(1)}y_{(1)})^{[2]}S(x_{(1)}y_{(1)})^{[1]}\\ &= x_{(0)}y_{(0)}(S(y_{(1)})S(x_{(1)}))^{[2]}(S(y_{(1)})S(x_{(1)}))^{[1]}\\ &\overset{(1.52)}{=} x_{(0)}[y_{(0)}S(y_{(1)})^{[2]}]S(x_{(1)})^{[2]}S(x_{(1)})^{[1]}S(y_{(1)})^{[1]}\\ &\overset{(1.54)}{=} x_{(0)}S(x_{(1)})^{[2]}S(x_{(1)})^{[1]}[y_{(0)}S(y_{(1)})^{[2]}]S(y_{(1)})^{[1]} = \theta(x)\theta(y),\end{aligned}$$

θ is an algebra morphism. Moreover,

$$\begin{aligned}h^{[1]}\otimes\theta(h^{[2]}) &= h^{[1]}\otimes {h^{[2]}}_{(0)}S({h^{[2]}}_{(1)})^{[2]}S({h^{[2]}}_{(1)})^{[1]} \overset{(1.50)}{=} {h_{(1)}}^{[1]}\otimes[{h_{(1)}}^{[2]}S(h_{(2)})^{[2]}]S(h_{(2)})^{[1]}\\ &\overset{(1.55)}{=} {h_{(1)}}^{[1]}[{h_{(1)}}^{[2]}S(h_{(2)})^{[2]}]\otimes S(h_{(2)})^{[1]} \overset{(1.48)}{=} \varepsilon(h_{(1)})S(h_{(2)})^{[2]}\otimes S(h_{(2)})^{[1]}\\ &= S(h)^{[2]}\otimes S(h)^{[1]},\end{aligned} \tag{1.56}$$

so we conclude that

$$\begin{aligned}(\mathrm{id}_T\otimes \mathrm{id}_{T^{op}}\otimes\theta)\mu(x) &= (\mathrm{id}_T\otimes \mathrm{id}_{T^{op}}\otimes\theta)(x_{(0)}\otimes {x_{(1)}}^{[1]}\otimes {x_{(1)}}^{[2]}) = x_{(0)}\otimes {x_{(1)}}^{[1]}\otimes\theta({x_{(1)}}^{[2]})\\ &= x_{(0)}\otimes S(x_{(1)})^{[2]}\otimes S(x_{(1)})^{[1]}.\end{aligned}$$

Hence,

$$\begin{aligned}&(\mathrm{id}_T\otimes \mathrm{id}_{T^{op}}\otimes\theta\otimes \mathrm{id}_{T^{op}}\otimes \mathrm{id}_T)(\mu\otimes \mathrm{id}_{T^{op}}\otimes \mathrm{id}_T)\mu(x)\\ &= (\mathrm{id}_T\otimes \mathrm{id}_{T^{op}}\otimes\theta\otimes \mathrm{id}_{T^{op}}\otimes \mathrm{id}_T)(\mu\otimes \mathrm{id}_{T^{op}}\otimes \mathrm{id}_T)(\mathrm{id}_T\otimes\gamma)(x_{(0)}\otimes x_{(1)})\\ &= (\mathrm{id}_T\otimes \mathrm{id}_{T^{op}}\otimes\theta)\mu(x_{(0)})\otimes\gamma(x_{(1)}) = x_{(0)}\otimes S(x_{(1)})^{[2]}\otimes S(x_{(1)})^{[1]}\otimes\gamma(x_{(2)});\end{aligned}$$

on the other hand,

$$\begin{aligned}(\mathrm{id}_T\otimes\mu^{op}\otimes \mathrm{id}_T)\mu(x) &= x_{(0)}\otimes\mu^{op}({x_{(1)}}^{[1]})\otimes {x_{(1)}}^{[2]}\\ &= x_{(0)}\otimes {x_{(1)}}^{[1]}{}_{(1)}^{[2]}\otimes {x_{(1)}}^{[1]}{}_{(1)}^{[1]}\otimes {x_{(1)}}^{[1]}{}_{(0)}\otimes {x_{(1)}}^{[2]}\\ &\overset{(1.51)}{=} x_{(0)}\otimes S(x_{(1)})^{[2]}\otimes S(x_{(1)})^{[1]}\otimes {x_{(2)}}^{[1]}\otimes {x_{(2)}}^{[2]}.\end{aligned}$$

Comparing these two equalities, we get (1.44). To prove (1.45), we first see that

$$\begin{aligned}\rho\theta(x) &= \rho([x_{(0)}S(x_1)^{[2]}]S(x_{(1)})^{[1]}) \overset{(1.54)}{=} x_{(0)}S(x_{(1)})^{[2]}\rho(S(x_{(1)})^{[1]})\\ &= x_{(0)}S(x_{(1)})^{[2]}S(x_{(1)})^{[1]}{}_{(0)} \otimes S(x_{(1)})^{[1]}{}_{(1)}\\ &\overset{(1.51)}{=} x_{(0)}S(x_{(1)})_{(2)}{}^{[2]}S(x_{(1)})_{(2)}{}^{[1]} \otimes S(S(x_{(1)})_{(1)})\\ &= x_{(0)}S(x_{(1)})^{[2]}S(x_{(1)})^{[1]} \otimes S^2(x_{(2)}) = \theta(x_{(0)}) \otimes S^2(x_{(2)})\end{aligned} \tag{1.57}$$

and therefore

$$\begin{aligned}(\theta\otimes\theta\otimes\theta)\mu(x) = \theta(x_{(0)}) \otimes \theta(x_{(1)}{}^{[1]}) \otimes \theta(x_{(1)}{}^{[2]}) &\overset{(1.56)}{=} \theta(x_{(0)}) \otimes \theta(S(x_{(1)})^{[2]}) \otimes S(x_{(1)})^{[1]}\\ &\overset{(1.56)}{=} \theta(x_{(0)}) \otimes S^2(x_{(1)})^{[1]} \otimes S^2(x_{(1)})^{[2]} = \theta(x_{(0)}) \otimes \gamma(S^2(x_{(1)}))\\ &\overset{(1.57)}{=} \theta(x)_{(0)} \otimes \gamma(\theta(x)_{(1)}) = \mu\theta(x).\end{aligned}$$

This proves that θ is a Grunspan map. □

Under conditions of faithful flatness, we have thus shown that

Quantum torsors $\Leftrightarrow$ Hopf Galois objects.

Moreover, if T is a quantum torsor, by Theorem 1.39, it is a faithfully flat right H-Galois object. But by Theorem 1.42, every faithfully flat right H-Galois object is a quantum torsor with Grunspan map. Hence, we have the following.

COROLLARY 1.43 ([SCH03, COROLLARY 3.6]). *Every quantum torsor has a Grunspan map.*

Now we present some examples from [Gru03]. Some of them evidence that this new perspective of Hopf Galois objects may include examples not studied as such before.

EXAMPLE 1.25 (HOPF ALGEBRAS). Let H be a K-Hopf algebra. By taking $\mu = (\mathrm{id}_H \otimes S \otimes \mathrm{id}_H)\Delta_2$, H becomes a K-torsor. Indeed, for every $h \in H$,

$$\begin{aligned}[(\mu\otimes \mathrm{id}_{H^{op}}\otimes \mathrm{id}_H)\mu](h) &= (\mu\otimes \mathrm{id}_{H^{op}}\otimes \mathrm{id}_H)(h_{(1)}\otimes S(h_{(2)})\otimes h_{(3)})\\ &= h_{(1)(1)}\otimes S(h_{(1)(2)})\otimes h_{(1)(3)}\otimes S(h_{(2)})\otimes h_{(3)}\\ &= h_{(1)}\otimes S(h_{(2)})\otimes h_{(3)}\otimes S(h_{(4)})\otimes h_{(5)}\\ &= h_{(1)}\otimes S(h_{(2)})\otimes h_{(3)(1)}\otimes S(h_{(3)(2)})\otimes h_{(3)(3)}\\ &= (\mathrm{id}_H\otimes \mathrm{id}_{H^{op}}\otimes\mu)(h_{(1)}\otimes S(h_{(2)})\otimes h_{(3)}) = [(\mathrm{id}_H\otimes \mathrm{id}_{H^{op}}\otimes\mu)\mu](h),\end{aligned}$$

which proves commutativity of the left diagram in (1.43). Similarly,

$$\begin{aligned}[(\mathrm{id}_H\otimes m)\mu](h) &= (\mathrm{id}_H\otimes m)(h_{(1)}\otimes S(h_{(2)})\otimes h_{(3)}) = h_{(1)}\otimes S(h_{(2)})h_{(3)}\\ &= h_{(1)}\otimes\varepsilon(h_{(2)}) = h_{(1)}\varepsilon(h_{(2)})\otimes 1 = h\otimes 1,\\ [(m\otimes \mathrm{id}_H)\mu](h) &= (m\otimes \mathrm{id}_H)(h_{(1)}\otimes S(h_{(2)})\otimes h_{(3)}) = h_{(1)}S(h_{(2)})\otimes h_{(3)}\\ &= \varepsilon(h_{(1)})\otimes h_{(2)} = 1\otimes\varepsilon(h_{(1)})h_{(2)} = 1\otimes h,\end{aligned}$$

showing the commutativity of the left diagram in (1.43). Moreover, since S is an anti-morphism

$$\begin{aligned}\mu(S(h)) &= (\mathrm{id}_H \otimes S \otimes \mathrm{id}_H)\Delta_2(S(h)) = (\mathrm{id}_H \otimes S \otimes \mathrm{id}_H)(S(h_{(3)}) \otimes S(h_{(2)}) \otimes S(h_{(1)})) \\ &= S(h_{(3)}) \otimes S^2(h_{(2)}) \otimes S(h_{(1)});\end{aligned}$$

hence,

$$\begin{aligned}\theta(h) &= h^{(1)}h^{(2)(3)}h^{(2)(2)}h^{(2)(1)}h^{(3)} = h_{(1)}S(h_{(2)})S^2(h_{(3)})S(h_{(4)})h_{(5)} \\ &= \varepsilon(h_{(1)})S(S(h_{(2)}))\varepsilon(h_{(3)}) = S^2(\varepsilon(h_{(1)})h_{(2)})\varepsilon(h_{(3)}) = S^2(h_1)\varepsilon(h_{(2)}) = S^2(h).\end{aligned}$$

Thus, $\theta = S^2$.

EXAMPLE 1.26 (SIMPLE ALGEBRAIC FIELD EXTENSIONS). Recall that a simple field extension E of a field $\Bbbk$ is one obtained by the adjunction of a single element, i.e., $E = \Bbbk(\alpha)$; in such a case, α is called primitive. It is known that, if α is algebraic over $\Bbbk$, then

$$E = \Bbbk(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \Bbbk[x],\, g(\alpha) \neq 0 \right\} \cong \Bbbk[x]/\langle q_\alpha(x) \rangle,$$

where $\Bbbk[x]$ is the classical univariate polynomial algebra over $\Bbbk$ and $q_\alpha(x)$ is the minimal polynomial of α over $\Bbbk$, i.e., the unique monic $\Bbbk$-polynomial of smallest degree satisfied by α (cf. [Rom06, Theorem 2.4.1]). Moreover, if $d = \mathrm{dg}(q_\alpha(x))$, then the set $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a $\Bbbk$-basis for E.

Suppose that $\Bbbk \subset E$ is a Galois extension of fields. Then, if $G = \{g_1, \ldots, g_n\}$ is the associated Galois group and $\{p_1, \ldots, p_n\} \subset \Bbbk^G$ is the dual basis, by Theorem 1.14, we known that the Galois map $\beta : E \otimes E \to E \otimes \Bbbk^G$, given by

$$F \otimes G \mapsto \sum_{i=1}^{n} F g_i(G) \otimes p_i, \qquad \text{for all } F, G \in E,$$

is bijective. Notice that the simple extension

$$E(\gamma) = \Bbbk(\alpha)(\gamma) = \Bbbk(\alpha, \gamma) = \left\{ \frac{f(\alpha, \gamma)}{g(\alpha, \gamma)} : f, g \in \Bbbk[x, y],\, g(\alpha, \beta) \neq 0 \right\}$$

can be identified with the algebra $E \otimes E$ in such a way that $\alpha \mapsto \alpha \otimes 1$ and $\gamma \mapsto 1 \otimes \alpha$. Then, clearly the inverse of $1_E \otimes p_k$ by β is

$$P_k := \prod_{j \neq k} \frac{\beta - g_j(\alpha)}{g_k(\alpha) - g_j(\alpha)}, \qquad \text{for all } k = 1, \ldots, n.$$

Indeed, having in mind the identification, for all $1 \leq k \leq n$,

$$\begin{aligned}\beta(P_k) &= \sum_{i=1}^{n} \prod_{j \neq k} \frac{1 g_i(\alpha) - g_j(\alpha) g_i(1)}{g_k(\alpha) g_i(1) - g_j(\alpha) g_i(1)} \otimes p_i = \sum_{i=1}^{n} \prod_{j \neq k} \frac{g_i(\alpha) - g_j(\alpha)}{g_k(\alpha) - g_j(\alpha)} \otimes p_i \\ &= \prod_{j \neq k} \frac{g_k(\alpha) - g_j(\alpha)}{g_k(\alpha) - g_j(\alpha)} \otimes p_k = 1_E \otimes p_k.\end{aligned}$$

Hence, following the proof of Theorem 1.42, we know that the map $\mu : E \to E \otimes E \otimes E$, given by

$$F \mapsto \sum_{i=1}^{n} g_i(F) \otimes P_i, \qquad \text{for all } F \in E,$$

makes E into a $\Bbbk$-torsor.

EXAMPLE 1.27 (NON-COMMUTATIVE QUANTUM TORSOR WITH NO CHARACTER). For a fixed non-negative integer n, suppose that the field $\Bbbk$ contains a n-th primitive root of unity $q \neq 1$. For any $\alpha, \beta \in \Bbbk^{\times}$, the $\Bbbk$-algebra generated by the elements x and y together with the relations

$$x^n = \alpha, \qquad y^n = \beta \qquad \text{and} \qquad xy = qyx,$$

is called the *non-commutative algebra without character* $A^{(n)}_{\alpha,\beta}$. It is known that this algebra is a non-trivial cyclic algebra and $\dim_{\Bbbk} A^{(n)}_{\alpha,\beta} = n^2$. If $n = 2$, it is an algebra of quaternions (cf. [Gru03, Example 2.8]).

Taking $T = A^{(n)}_{\alpha,\beta}$, we define $\mu : T \to T \otimes T^{op} \otimes T$ as

$$\mu(x) = x \otimes x^{-1} \otimes x \qquad \text{and} \qquad \mu(y) = y \otimes y^{-1} \otimes y.$$

Since

$$\begin{aligned}
(\mathrm{id}_T \otimes \mathrm{id}_{T^{op}} \otimes \mu)\mu(x) &= (\mathrm{id}_T \otimes \mathrm{id}_{T^{op}} \otimes \mu)(x \otimes x^{-1} \otimes x) = x \otimes x^{-1} \otimes x \otimes x^{-1} \otimes x \\
&= (\mu \otimes \mathrm{id}_{T^{op}} \otimes \mathrm{id}_T)(x \otimes x^{-1} \otimes x) = (\mu \otimes \mathrm{id}_{T^{op}} \otimes \mathrm{id}_T)\mu(x), \\
(\mathrm{id}_T \otimes m)\mu(x) &= (\mathrm{id}_T \otimes m)(x \otimes x^{-1} \otimes x) = x \otimes 1, \\
(m \otimes \mathrm{id}_T)\mu(x) &= (m \otimes \mathrm{id}_T)(x \otimes x^{-1} \otimes x) = 1 \otimes x,
\end{aligned}$$

and the sames calculations are valid for y, $T = A^{(n)}_{\alpha,\beta}$ together with μ is a quantum $\Bbbk$-torsor.

Grunspan found that, if the base ring is a field, then we can attach two Hopf algebras to any quantum torsor.

THEOREM 1.44 (RECONSTRUCTION THEOREM, [GRU03, THEOREM 2.10]). *Let T be a quantum $\Bbbk$-torsor with associated map $\mu : T \to T \otimes T^{op} \otimes T$ and Grunspan map $\theta : T \to T$. Put*

$$H_l(T) := \{z \in T \otimes T^{op} : (\mathrm{id}_T \otimes \mathrm{id}_{T^{op}} \otimes \theta \otimes \mathrm{id}_{T^{op}})(\mu \otimes \mathrm{id}_{T^{op}})(z) = (\mathrm{id}_T \otimes \mu^{op})(z)\}. \tag{1.58}$$

Then, the following assertions hold:

(i) *If $z \in H_l(T)$, then both $m_T(z)$ and $m_{T^{op}}(\theta \otimes \mathrm{id}_{T^{op}})(z)$ are equal to a common scalar denoted by $\varepsilon(z)1_T$.*

(ii) *If $z \in H_l(T)$, then $\Delta(z) := (\mu \otimes \mathrm{id}_{T^{op}})(z) \in H_l(T) \otimes H_l(T)$.*

(iii) *By defining $m_{H_l(T)}$ as the restriction of $m_T \otimes m_T^{op}$ to $H_l(T)$ and $u_{H_l(T)} : \Bbbk \to H_l(T)$ as $u_{H_l(T)}(1) = 1_T \otimes 1_T$, $H_l(T)$ becomes a bialgebra.*

(iv) *$\mathrm{Im}(u_T) \subset H_l(T) \otimes T$ and $\gamma_T := \mu : T \to H_l(T) \otimes T$ embeds T with a left $H_l(T)$-comodule structure.*

Moreover, if we set $S_{H_l(T)}(z) := \tau_T(\theta \otimes \mathrm{id}_{T^{op}})(z)$, *for all* $z \in H_l(T)$, *then* $\mathrm{Im}(S_{H_l(T)}) \subset H_l(T)$ *and hence* $H_l(T)$ *is a Hopf algebra.*

In fact, [Gru03] proves the theorem also for $\Bbbk[[x]]$-torsors, providing T is topologically free over $\Bbbk[[x]]$. Moreover, it is asseverated that the theorem can be extended to torsors over principal ideal domains, although we were not able to find a proof of such assertion.

Similarly, for every $\Bbbk$-torsor T, we can define a Hopf algebra structure on the set

$$H_r(T) = \{z \in T^{op} \otimes T : (\mathrm{id}_{T^{op}} \otimes \theta \otimes \mathrm{id}_{T^{op}} \otimes \mathrm{id}_T)(\mathrm{id}_{T^{op}} \otimes \mu)(z) = (\mu^{op} \otimes \mathrm{id}_T)(z)\}. \tag{1.59}$$

We also have $\mathrm{Im}(\mu) \subset T \otimes H_r(T)$ and hence the map $\delta_T := \mu = T \to T \otimes H_r(T)$ equips T with an right $H_r(T)$-comodule algebra structure. Moreover, the commutativity of the left diagram in Definition 1.39 implies that the two structures of left $H_l(T)$-comodule algebra and right $H_r(T)$-comodule algebra are compatible. Therefore, we get the following corollary.

COROLLARY 1.45 ([GRU03, COROLLARY 2.17]). *Let* T *be a quantum* $\Bbbk$*-torsor. Then* T *is a* $H_l(T)$*-*$H_r(T)$*-bicomodule algebra of* $\Bbbk$.

In [Gru03, Corollary 4.13] is shown that, in fact, T is a $H_l(T)$-$H_r(T)$-biGalois object. some properties of $H_l(T)$ and $H_r(T)$ and the explicit calculation of them for the examples listed before can be found after such corollary.

Roughly speaking, the next result establishes that these Hopf algebras attached to quantum torsors and the ones find in Hopf biGalois extensions (cf. [Sch96]) are the same. Since the proof uses either Hopf biGalois theory, or Miyashita-Ulbrich techniques (cf. [Sch02, §4]), and those topics are not covered in this document, we shall omit it.

PROPOSITION 1.46 ([SCH02, PROPOSITION 3.4]). (i) *Let* T *be a faithfully flat* H*-Galois object and consider the quantum torsor structure associate to it as in Theorem 1.42. Then* $H_r(T) \cong H$ *and* $H_l(T) = (T \otimes T)^{coH}$.

(ii) *If* T *is a quantum torsor, then the quantum torsor associated as in Theorem 1.42 to the* $H_r(T)$*-Galois object* T *coincides with* T.

We end this section by discussing a generalization of quantum torsors proposed by Schauenburg. For that, let B be a K-algebra and $B \subset T$ an algebra extension such that T is a faithfully flat K-module. Since $T \otimes_B T$ is obviously a B-B-bimodule, we can consider the centralizer

$$C_B(T \otimes_B T) := \{t \in T \otimes_B T : b \cdot t = t \cdot b, \text{for all } b \in B\}.$$

We can endow this module with an algebra structure.

LEMMA 1.47. *The centralizer* $C_B(T \otimes_B T)$ *is a* K*-algebra with multiplication given by*

$$(x \otimes y)(z \otimes w) := zx \otimes yw, \qquad \textit{for all } x \otimes y, z \otimes w \in C_B(T \otimes_B T),$$

and unit $1_T \otimes 1_T$.

Proof. If $x\otimes y, z\otimes w \in C_B(T\otimes_B T)$, then

$$\begin{aligned} b[(x\otimes y)(z\otimes w)] &= b(zx\otimes yw) = bzx\otimes yw = (x\otimes y)(bz\otimes w) = (x\otimes y)[b(x\otimes w)] \\ &= (x\otimes y)[(z\otimes w)b] = (x\otimes y)(z\otimes wb) = zx\otimes ywb = (zx\otimes yw)b \\ &= [(x\otimes y)(z\otimes w)]b. \end{aligned}$$

Thus, $C_B(T\otimes_B T)$ is indeed closed under this operation. The other properties are immediate to check. □

DEFINITION 1.41 (GENERALIZED QUANTUM TORSOR, [SCH04, DEFINITION 2.8.1]). Let B be a K-algebra and $B\subset T$ an algebra extension such that T is a faithfully flat K-module. A *(generalized) quantum B-torsor* structure on T is a map $\mu: T\to T\otimes C_B(T\otimes_B T)$ such that, if the induced map $\mu_0: T\to T\otimes T\otimes_B T$ is denoted by $\mu_0(x) := x^{(1)}\otimes x^{(2)}\otimes x^{(3)}$, then the following relations hold:

$$x^{(1)}x^{(2)}\otimes x^{(3)} = 1\otimes x \in T\otimes_B T,$$
$$x^{(1)}\otimes x^{(2)}x^{(3)} = x\otimes 1 \in T\otimes T,$$
$$\mu(b) = b\otimes 1\otimes 1,\ \forall b\in B, \tag{1.60}$$
$$\mu(x^{(1)})\otimes x^{(2)}\otimes x^{(3)} = x^{(1)}\otimes x^{(2)}\otimes \mu(x^{(3)}) \in T\otimes T\otimes_B \otimes T\otimes_B T. \tag{1.61}$$

Notices that (1.60) implies that μ is a left B-module map and hence the relation actually (1.61) makes sense. This generalization of quantum torsor also induces a descend datum.

LEMMA 1.48 ([SCH04, LEMMA 2.8.3]). *Let T be a quantum B-torsor in the sense of Definition 1.41. Then*

$$D(x\otimes y) = xy^{(1)}\otimes y^{(2)}\otimes y^{(3)}$$

defines a T/K-descent datum on $T\otimes_B T$. Moreover, it satisfies

$$(T\otimes D)\mu(x) = x^{(1)}\otimes 1\otimes x^{(2)}\otimes x^{(3)}$$

and $D(T\otimes_B T)\subset T\otimes C_B(T\otimes_B T)$.

Proof. The calculations are completely similar to those made in the proof of Lemma 1.38. The only new part is the last one, which is immediately obtained from noticing that, by definition, $y^{(2)}\otimes y^{(3)}$ is in the centralizer. □

Recall that for an arbitrary descent datum D on $\mathrm{DD}(S/R)$ over M, Lemma 1.37 gives an associated R-module ${}^DM = \{m\in M : D(m) = 1\otimes m\}$. From the above, we conclude that in our setup ${}^D(T\otimes_B T)\subset C_B(T\otimes_B T)$. Hence, we have the following result, which generalizes Theorem 1.39.

THEOREM 1.49 ([SCH04, THEOREM 2.8.4]). *Let T be a quantum B-torsor such that T is faithfully flat as right B-module. If*

$$H := {}^D(T\otimes_B T) = \{x\otimes y\in T\otimes_B T : xy^{(1)}\otimes y^{(2)}\otimes y^{(3)} = 1\otimes x\otimes y\},$$

then the following assertions hold:

(i) *H is a K-flat Hopf algebra. The algebra structure is that of a subalgebra of $C_B(T \otimes_B T)$; comultiplication and counit are given by*

$$\Delta(x \otimes y) = x \otimes y^{(1)} \otimes y^{(2)} \otimes y^{(3)} \qquad \text{and} \qquad \varepsilon(x \otimes y) = xy.$$

(ii) *T is a right H-comodule algebra with structure map given by $\rho = \mu$. Moreover, $T^{coH} = B$.*

(iii) *$B \subset T$ is a right H-Galois extension.*

Proof. Again, the calculations are not essentially different from the ones in Theorem 1.39, the only difference being is that, in this case, the assumption of faithful flatness of T_B is used to deduce, along the bijectivity of the Galois map $\beta : T \otimes_B T \to T \otimes H$, that H is a faithful flat K-module. □

Finally, we have the following result which, together with the previous one, establishes that

Generalized quantum torsors ⇔ Hopf Galois extensions,

provided conditions of faithful flatness.

THEOREM 1.50 ([SCH04, LEMMA 2.8.5]). *Let H be a faithfully flat K-Hopf algebra and $T^{coH} \subset T$ a faithfully flat right H-Galois extension. If $B := T^{coH}$, then T is a quantum B-torsor with associated map $\mu : T \to T \otimes C_B(T \otimes_B T)$ defined by*

$$\mu(x) = x_{(0)} \otimes {x_{(1)}}^{[1]} \otimes {x_{(1)}}^{[2]}, \qquad \text{for all } x \in T, \tag{1.62}$$

where $h^{[1]} \otimes h^{[2]} := \beta^{-1}(1 \otimes h) \in T \otimes_B T$, whit $\beta : T \otimes_B T \to T \otimes H$ the Galois map.

1.5 HOPF GALOIS SYSTEMS

Almost parallel to the develop of quantum torsors, [Bic03a] gave another formulation for non-commutative torsors. His approach was that of noticing that a classical torsor naturally gives rise to a grupoid with two objects. Although the axiomatic is slightly complicated, it is also more natural an easier to handle with.

DEFINITION 1.42 (HOPF GALOIS SYSTEM [BIC03A, DEFINITION 1.1]). A *K-Hopf Galois system* consists of four K-algebras (A, B, Z, T) satisfying the following axioms:

(HGS1) A and B are K-bialgebras,

(HGS2) Z is an A-B-bicomodule algebra with respective structure maps $\alpha_Z : Z \to A \otimes Z$ and $\beta_Z : Z \to Z \otimes B$.

(HGS3) There exist algebra morphisms $\gamma : A \to Z \otimes T$ and $\delta : B \to T \otimes Z$ such that the following

diagrams commute:

$$\begin{array}{ccc} Z & \xrightarrow{\alpha_Z} & A\otimes Z \\ {\scriptstyle\beta_Z}\downarrow & & \downarrow{\scriptstyle\gamma\otimes \mathrm{id}_Z} \\ Z\otimes B & \xrightarrow[\mathrm{id}_Z\otimes\delta]{} & Z\otimes T\otimes Z \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\Delta_A} & A\otimes A \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_A\otimes\gamma} \\ Z\otimes T & \xrightarrow[\alpha_Z\otimes\mathrm{id}_T]{} & Z\otimes T\otimes Z \end{array} \qquad \begin{array}{ccc} B & \xrightarrow{\Delta_B} & B\otimes B \\ {\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle\delta\otimes\mathrm{id}_B} \\ T\otimes Z & \xrightarrow[\mathrm{id}_T\otimes\beta_Z]{} & T\otimes Z\otimes B \end{array}$$

(HGS4) There exists a K-linear map $S: T \to Z$ such that the following diagrams commute:

$$\begin{array}{ccccc} A & \xrightarrow{\varepsilon_A} & K & \xrightarrow{u_Z} & Z \\ {\scriptstyle\gamma}\downarrow & & & & \uparrow{\scriptstyle m_Z} \\ Z\otimes T & & \xrightarrow[\mathrm{id}_Z\otimes S]{} & & Z\otimes Z \end{array} \qquad \begin{array}{ccccc} B & \xrightarrow{\varepsilon_B} & K & \xrightarrow{u_Z} & Z \\ {\scriptstyle\delta}\downarrow & & & & \uparrow{\scriptstyle m_Z} \\ T\otimes Z & & \xrightarrow[S\otimes\mathrm{id}_Z]{} & & Z\otimes Z \end{array}$$

While keeping the convention in notation of Remark 15, we can extend somehow Sweedler's sigma notation to Hopf Galois systems, writing

$$\gamma(a) = a_Z \otimes a_T \qquad \text{and} \qquad \delta(b) = b_T \otimes b_Z, \qquad \text{for all } a \in A \text{ and } b \in B.$$

[Bic03a, Corollary 1.3] proves that, for any Hopf Galois system (A, B, Z, T), the bialgebras A and B are in fact Hopf algebras. Additionally, in [Bic03a, Corollary 1.10] is shown that $S: T \to Z^{op}$ is an algebra morphism.

For future reference in the calculations below, we state explicitly the commutativity of the diagrams in (HGS3) and (HGS4):

$$(\gamma\otimes \mathrm{id}_Z)\alpha_Z = (\mathrm{id}_Z\otimes\delta)\beta_Z, \tag{1.63}$$
$$(\mathrm{id}_A\otimes\gamma)\Delta_A = (\alpha_Z\otimes \mathrm{id}_T)\gamma, \tag{1.64}$$
$$(\delta\otimes \mathrm{id}_B)\Delta_B = (\mathrm{id}_T\otimes\beta_Z)\delta, \tag{1.65}$$
$$m_Z(\mathrm{id}_Z\otimes S)\gamma = u_Z\varepsilon_A, \tag{1.66}$$
$$m_Z(S\otimes \mathrm{id}_Z)\delta = u_Z\varepsilon_B. \tag{1.67}$$

The next result relates Hopf Galois systems with Hopf biGalois objects.

THEOREM 1.51 ([BIC03A, THEOREM 1.2]). *Let (A, B, Z, T) be a K-Hopf Galois system with Z faithfully flat over K. Then Z is an A-B-biGalois object.*

Proof. ($\Rightarrow$) By Remark 9, first we have to prove that the composition

$$\beta_l: \; Z\otimes Z \xrightarrow{\alpha_Z\otimes\mathrm{id}_Z} A\otimes Z\otimes Z \xrightarrow{\mathrm{id}_A\otimes m_Z} A\otimes Z$$

is bijective. For that, let $\eta_l : A \otimes Z \to Z \otimes Z$ be the map defined as the composition

$$\eta_l : \ A \otimes Z \xrightarrow{\gamma \otimes \mathrm{id}_Z} Z \otimes T \otimes Z \xrightarrow{\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z} Z \otimes Z \otimes Z \xrightarrow{\mathrm{id}_Z \otimes m_Z} Z \otimes Z.$$

Notice that, for all $a \in A$ and $z, w \in Z$ we have

$$\begin{aligned}
&(\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z)(\gamma \otimes \mathrm{id}_Z)(\mathrm{id}_A \otimes m_Z)(a \otimes z \otimes w) = (\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z)(\gamma \otimes \mathrm{id}_Z)(a \otimes zw) \\
&= (\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z)(a_Z \otimes a_T \otimes zw) = a_Z \otimes S(a_T) \otimes zw = (\mathrm{id}_Z \otimes \mathrm{id}_Z \otimes m_Z)(a_Z \otimes S(a_T) \otimes z \otimes w) \\
&= (\mathrm{id}_Z \otimes \mathrm{id}_Z \otimes m_Z)(\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z \otimes \mathrm{id}_Z)(a_Z \otimes a_T \otimes z \otimes w) \\
&= (\mathrm{id}_Z \otimes \mathrm{id}_Z \otimes m_Z)(\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z \otimes \mathrm{id}_Z)(\gamma \otimes \mathrm{id}_Z \otimes \mathrm{id}_Z)(a \otimes z \otimes w),
\end{aligned}$$

so

$$(\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z)(\gamma \otimes \mathrm{id}_Z)(\mathrm{id}_A \otimes m_Z) = (\mathrm{id}_Z \otimes \mathrm{id}_Z \otimes m_Z)(\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z \otimes \mathrm{id}_Z)(\gamma \otimes \mathrm{id}_Z \otimes \mathrm{id}_Z). \quad (1.68)$$

Hence,

$$\begin{aligned}
\eta_l \beta_l &= (\mathrm{id}_Z \otimes m_Z)(\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z)(\gamma \otimes \mathrm{id}_Z)(\mathrm{id}_A \otimes m_Z)(\alpha_Z \otimes \mathrm{id}_Z) \\
&\overset{(1.68)}{=} (\mathrm{id}_Z \otimes m_Z)(\mathrm{id}_Z \otimes m_Z \otimes \mathrm{id}_Z)(\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z \otimes \mathrm{id}_Z)(\mathrm{id}_Z \otimes \delta \otimes \mathrm{id}_Z)(\beta \otimes \mathrm{id}_Z) \\
&\overset{(1.67)}{=} (\mathrm{id}_Z \otimes m_Z)(\mathrm{id}_Z \otimes u_Z \varepsilon_B \otimes \mathrm{id}_Z)(\beta_Z \otimes \mathrm{id}_Z) \\
&\overset{(1.15)}{=} \mathrm{id}_{Z \otimes Z}.
\end{aligned}$$

Similarly, one can show that $\beta_l \eta_l = \mathrm{id}_{A \otimes Z}$ and hence β_l is bijective.

On the other hand, we also have to prove that the composition

$$\beta_r : \ Z \otimes Z \xrightarrow{\mathrm{id}_Z \otimes \beta_Z} Z \otimes Z \otimes B \xrightarrow{m_Z \otimes \mathrm{id}_B} Z \otimes B$$

is bijective. For that, we define $\eta_r : Z \otimes B \to Z \otimes Z$ as the composition

$$\eta_r : \ Z \otimes B \xrightarrow{\mathrm{id}_Z \otimes \delta} Z \otimes T \otimes Z \xrightarrow{\mathrm{id}_z \otimes S \otimes \mathrm{id}_Z} Z \otimes Z \otimes Z \xrightarrow{m_Z \otimes \mathrm{id}_Z} Z \otimes Z,$$

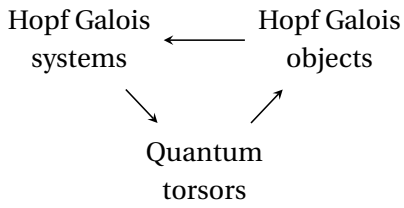
and similar to the first part, one can prove that η_r is the inverse of β_r.

Finally, since Z is K-faithfully flat, by Proposition 1.12, it is A-B-faithfully flat. □

The converse is proven using techniques of *Tannaka duality* (cf. [Sch92] and [Bic03a, Remark 1.9]).

THEOREM 1.52 ([BIC03A, COROLLARY 1.8]). *Let A be a faithfully flat K-Hopf algebra and Z a faithfully flat left A-Galois object. Then there exists a Hopf algebra B and an algebra T such that (A, B, Z, T) is a Hopf Galois system.*

Hence, with certain assumptions of faithful flatness, the following diagram is commutative:



(1.69)

The explicit equivalence between quantum torsors and Hopf Galois systems is explored in [Gru03, §4.2] and will be addressed in Section 3.2. We only mention the following result.

THEOREM 1.53 ([GRU03, THEOREM 4.2]). *Let (A,B,Z,T) be a K-Hopf-Galois system. Then $\mu : Z \to Z \otimes Z^{op} \otimes Z$ given by*

$$\mu = (\mathrm{id}_Z \otimes S \otimes \mathrm{id}_Z)(\gamma \otimes \mathrm{id}_Z)\alpha_Z$$

makes Z into a quantum K-torsor.

Finally, we address some examples of Hopf Galois systems, which are adapted from [Bic03a] and [Sch96].

EXAMPLE 1.28 (HOPF ALGEBRAS). Let H be a K-Hopf algebra. If we put $A = B = Z = T = H$, $\alpha_Z = \beta_Z = \gamma = \delta = \Delta_H$ and $S = S_H$, then (A,B,Z,T) is a Hopf Galois system. Indeed, (1.63)-(1.65) correspond to the coassociativity and (1.66)-(1.67) to the main property of the antipode.

EXAMPLE 1.29 (HOPF ALGEBRAS TWISTED BY 2-COCYCLES). Let H be a faithfully flat K-Hopf algebra. Using the universal property of the tensor product, for any $\sigma \in \mathrm{Hom}_K(H \otimes H, K)$, since it corresponds to an unique bilinear K-form, we shall write

$$\sigma(h \otimes k) = \sigma(h,k), \qquad \text{for all } h,k \in H.$$

Notice that, since $H \otimes H$ is a coalgebra and K is an algebra, $\mathrm{Hom}_K(H \otimes H, K)$ is also an algebra with the convolution product.

Following [Doi93], we say that $\sigma : H \otimes H \to K$ is a 2-*cocycle* if σ is a convolution invertible K-linear map satisfying

$$\sigma(g_{(1)},h_{(1)})\sigma(g_{(2)}h_{(2)},k) = \sigma(h_{(1)},k_{(1)})\sigma(g,h_{(2)}k_{(2)}),$$
$$\sigma(h,1) = \sigma(1,h) = \varepsilon(h)1,$$

for all $g,h,k \in H$. If $\overline{\sigma}$ denotes the convolution inverse of σ, by [Doi93, Theorem 1.6], it satisfies

$$\overline{\sigma}(f_{(1)}g_{(1)},h)\overline{\sigma}(f_{(2)},g_{(2)}) = \overline{\sigma}(f,g_{(1)}h_{(1)})\overline{\sigma}(g_{(2)}h_{(2)})$$
$$\overline{\sigma}(h,1) = \overline{\sigma}(1,h) = \varepsilon(h)1,$$

for all $f,g,h \in H$.

For a fixed 2-cocycle σ over H, we consider a new multiplication over the K-module H, given by

$$h \cdot_\sigma k := \sigma(h_{(1)},k_{(1)})h_{(2)}k_{(2)}, \qquad \text{for all } h,k \in H.$$

This new algebra is denoted by ${}_\sigma H$. Similarly, another possible product for H is

$$h \cdot_{\overline{\sigma}} k := \overline{\sigma}(h_{(2)}, k_{(2)}) h_{(1)} k_{(1)}, \qquad \text{for all } h, k \in H,$$

and the induced algebra is denoted by $H_{\overline{\sigma}}$. Notice that $H_{\overline{\sigma}}$ is a H-comodule algebra with structure map $\rho_l = \Delta_H$.

Finally, we can also induce a new Hopf algebra ${}_\sigma H_{\overline{\sigma}}$, which is isomorphic to H as coalgebra, with multiplication

$$k \cdot h := \sigma(h_{(1)}, k_{(1)}) \overline{\sigma}(h_{(3)}, k_{(3)}) h_{(2)} k_{(2)}, \qquad \text{for all } h, k \in H,$$

and antipode

$$S^\sigma(h) := \sigma(h_{(1)}, S(h_{(2)})) \overline{\sigma}(S(h_{(4)}), h_{(5)}) S(h_{(3)}), \qquad \text{for all } h \in H.$$

Notice that $H_{\overline{\sigma}}$ is a right ${}_\sigma H_{\overline{\sigma}}$-comodule algebra with structure map $\rho_r = \Delta$. Moreover, $H_{\overline{\sigma}}$ is a H-${}_\sigma H_{\overline{\sigma}}$-bicomodule algebra. The details of these constructions can be found in [Doi93, §2] and [Sch96, §3].

[Bic03a, Proposition 2.1] and [Doi90, Theorem 1.6.(a5)] show that $(H, {}_\sigma H_{\overline{\sigma}}, H_{\overline{\sigma}}, {}_\sigma H)$ is a Hopf Galois system.

EXAMPLE 1.30 (HOPF ALGEBRAS OF A NON-DEGENERATE BILINEAR FORM). Let $\Bbbk$ be an algebraically closed field and $n, m > 1$. For two fixed invertible matrices $E_{m\times m}$ and $F_{n\times n}$, we denote by $\mathscr{B}(E,F)$ the $\Bbbk$-algebra generated by $\{x_{ij} : 1 \le i \le m,\ 1 \le j \le n\}$ together with the relations

$$F^{-1t} X E X = I_n \qquad \text{and} \qquad X F^{-1t} X E = I_m,$$

where X is the matrix (x_{ij}) and I_n and I_m are the identity matrices of size n and m, respectively.

For the particular case $n = m$ and $E = F$ we simply write $\mathscr{B}(E)$; this (Hopf) algebra was introduced by [DVL90] and turns out to be the function algebra on the quantum (symmetry) group of a non-degenerate bilinear form (cf. [Bic03b, §2]). For any matrix $A = (a_{ij})$ over $\mathscr{B}(E)$, the comultiplication, counit and antipode are given by

$$\Delta(a_{ij}) = \sum_{k=1}^{n} a_{ik} \otimes a_{ik}, \qquad \varepsilon(a_{ij}) = \delta_{ij} \qquad \text{and} \qquad S(A) = E^{-1t} A E,$$

where δ_{ij} denotes the Kronecker delta.

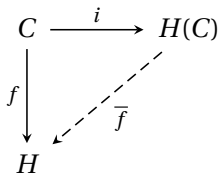
[Bic03a, Proposition 3.1] proves that, if $\operatorname{tr}(E^t E^{-1}) = \operatorname{tr}(F^t F^{-1})$, then

$$(\mathscr{B}(E), \mathscr{B}(F), \mathscr{B}(E,F), \mathscr{B}(F,E))$$

is a Hopf Galois system. Without the assumption on the traces, [Bic03b, Proposition 3.3] verify directly that $\mathscr{B}(E,F)$ is a $\mathscr{B}(E)$-$\mathscr{B}(F)$-biGalois object.

EXAMPLE 1.31 (FREE HOPF ALGEBRAS GENERATED BY DUAL MATRIX COALGEBRAS). Let C be a K-coalgebra. We say that a K-Hopf algebra $H(C)$ is a *free Hopf algebra generated by* C if there exists a coalgebra map $i : C \to H(C)$ such that the following universal property is satisfied: *for any K-Hopf algebra H A and any coalgebra morphism $f : C \to H$ there exists an unique Hopf*

algebra morphism $\overline{f} : H(C) \to H$ such that the following diagram is commutative:



From the above follows that $H(C)$ is unique up to isomorphism. The existence of such free Hopf algebra is shown in [Tak71, §1] with an explicit construction of $H(C)$ as follows. Let $\{V_i\}_{i\geq 0}$ be the sequence of coalgebras

$$V_0 := C \qquad \text{and} \qquad V_{i+1} := V_i^{op},\ i \geq 0.$$

Let $V := \bigoplus_{i\geq 0} V_i$ be their direct sum, which is also a coalgebra via the induced pointwise operations. Considering the tensor algebra $T(V)$, we define the coalgebra map $S : V \to V^{op}$ by

$$(x_0, x_1, \ldots) \mapsto (0, x_0, x_1, \ldots),$$

which induces a bialgebra map $S : T(V) \to T(V)^{op}$. Now, let

$$I = \langle x_{(1)}S(x_{(2)}) - \varepsilon(x)1, S(x_{(1)})x_{(2)} - \varepsilon(x)1 : x \in V\rangle.$$

One can check that I is in fact a Hopf ideal of $T(V)$, and therefore $H(C) := T(V)/I$ is a Hopf algebra with antipode induced by S.

A particular case of the above is when $C = (M_n(\Bbbk))^*$, where $M_n(\Bbbk)$ denotes the algebra of $n \times n$ matrices over $\Bbbk$. In such case, $H(C)$ is denoted by $H(n)$ and corresponds to the $\Bbbk$-algebra generated by $\{u_{ij}^{(\alpha)} : 1 \leq i, j \leq n, \alpha \in \mathbb{N}\}$ satisfiying the relations

$$(u^{(\alpha)})^t u^{(\alpha+1)} = I_n = u^{(\alpha+1)}(u^{(\alpha)})^t,$$

where $u^{(\alpha)}$ is the $n \times n$ matrix $(u_{ij}^{(\alpha)})$ (cf. [DW96, Theorem 3.1]). More generally, for $m, n \geq 1$, we consider the algebra $H(m, n)$ as that generated by $\{u_{ij}^{(\alpha)} : 1 \leq i \leq m, 1 \leq j \leq n, \alpha \in \mathbb{N}\}$ together with the relation

$$(u^{(\alpha)})^t u^{(\alpha+1)} = I_m \qquad \text{and} \qquad u^{(\alpha+1)}t(u^{(\alpha)}) = I_n,$$

where $u^{(\alpha)}$ is the $n \times m$ matrix $(u_{ij}^{(\alpha)})$.

[Bic03a, Proposition 5.2] proves that, for $m, n \geq 2$, $(H(m), H(n), H(m, n), H(n, m))$ is a Hopf Galois system.

Hopf Galois systems can be also constructed for some particular cosovereign Hopf algebra (cf. [Bic01] and [Bic03a, §4]).

CHAPTER 2

FAMILIES OF NON-COMMUTATIVE RINGS

In the last century, non-commutative rings and algebras have appeared in almost every subject of research – not only mathematical but also physical. Therefore, the study of certain algebras given by their generators and relations has become useful. However, within a more practical approach, some general families of non-commutative rings have been defined and studied along the years.

Although these collections do not cover, in general, every remarkable example, most of such families contain a notorious amount of distinguished algebras, even having the case that one object can be endowed with two or more different structures, as we shall relate in the examples. In this chapter we will address several of such families of rings, most of them having a polynomial behavior.

Quite popular for describing a large number of algebras and for having a pioneering role in the systematic research of non-commutative rings, in Section 2.1 we star reviewing the skew polynomial rings. Section 2.2 is dedicated to the PBW extensions which comprehend rings with the PBW basis property, while Section 2.3 addresses a generalizations of such setup. Finally, in Section 2.4 we present a generalization of enveloping universal algebras over Lie algebras.

2.1 SKEW POLYNOMIAL RINGS

Introduced by [Ore33], skew polynomial rings are distinguished by their elements, which have a polynomial aspect but not necessarily the variable is assumed to commute with coefficients. For such "commutation" to take place, certain rule involving an endomorphism and a derivation of the ground ring is established.

DEFINITION 2.1 ([MR01, 1.2.1]). Let R be a ring and $\sigma : R \to R$ an endomorphism. An additive map $\delta : R \to R$ is called a *σ-derivation of R*, if

$$\delta(rs) = \sigma(r)\delta(s) + \delta(r)s, \qquad \text{for all } r, s \in R.$$

Notice that, in particular, $\delta(1) = \delta(1 \cdot 1) = \sigma(1)\delta(1) + \delta(1)1 = 2\delta(1)$, whence $\delta(1) = 0$.

DEFINITION 2.2 (SKEW POLYNOMIAL RING, [MR01, 1.2.3]). Let R be a ring, $\sigma : R \to R$ an endomorphism and $\delta : R \to R$ a σ-derivation of R. A ring A such that

(O1) A contains R as a proper subring,

(O2) There is an element $x \in A$ such that A is a left free R-module with basis $\{1, x, x^2, x^3, \ldots\}$,

(O3) $xr = \sigma(r)x + \delta(r)$, for all $r \in R$,

is called a *skew polynomial ring over* R. In this case we write $A := R[x; \sigma, \delta]$.

Skew polynomial rings are also known as *Ore extensions*.

REMARK 16. There are some constructive proofs showing the existence of skew polynomial rings (cf. [GW04, Proposition 2.3] or [Lez19c, §1.1]), which verify the ring structure of $A = R[x; \sigma, \delta]$ not falling in the tedious calculations of a direct proof.

Moreover, such constructions guarantee that, given any ring R, any ring endomorphism σ of R and any σ-derivation of R, there always will exist the skew polynomial ring $R[x; \sigma, \delta]$.

For a fixed ring R, let $R[x; \sigma, \delta]$ be a skew polynomial ring over R. From (O3) it is natural to ask for a general formula to express $x^i r$ ($i \in \mathbb{N}$ and $r \in R$) as a *polynomial* with *left coefficients*. Nevertheless, those calculations can be tricky; for instance, with $i = 3$,

$$x^3 r = \sigma^3(r)x^3 + [\delta\sigma^2(r) + \sigma\delta\sigma(r) + \sigma^2\delta(r)]x^2 + [\delta^2\sigma(r) + \delta\sigma\delta(r) + \sigma\delta^2(r)]x + \delta^3(r).$$

However, using an inductive argument, it can be shown that the *multiplication rule* can be written as follows. Given $r \in R$ and $i, k \in \mathbb{N}$, we denote by $W[\delta^k \sigma^{i-k}](r)$ the evaluation of r in the function given by the sum of all possible *words* that can be constructed with the alphabet formed by k-times the symbol δ and $(i-k)$-times the symbol σ, where the concatenation is understood as the composition of functions. For instance, if $k = 2$ and $i = 5$ we get

$$\begin{aligned} W[\delta^2\sigma^3](r) = {} & \delta^2\sigma^3(r) + \delta\sigma\delta\sigma^2(r) + \delta\sigma^2\delta\sigma(r) + \delta\sigma^3\delta(r) + \sigma\delta^2\sigma^2(r) \\ & + \sigma\delta\sigma\delta\sigma(r) + \sigma\delta\sigma^2\delta(r) + \sigma^2\delta^2\sigma(r) + \sigma^2\delta\sigma\delta(r) + \sigma^3\delta^2(r). \end{aligned}$$

In the general case, if $r \in R$ and $i \in \mathbb{N}$, the following formula holds:

$$x^i r = \sum_{k=0}^{i} W[\delta^k \sigma^{i-k}](r) x^{i-k}. \tag{2.1}$$

Moreover, if $r, s \in R$ and $i, j \in \mathbb{N}$, then:

$$(rx^i)(sx^j) = r \sum_{k=0}^{i} W[\delta^k \sigma^{i-k}](s) x^{i+j-k}. \tag{2.2}$$

The above shows that, in the ring $A = R[x; \sigma, \delta]$, the product of two *terms* rx^n and sx^m is not necessarily another term, yet in general it will be a polynomial. However, by (O2), it is quite clear

that every element $p \in R[x;\sigma,\delta]$ can be uniquely written as

$$p = \sum_{i=0}^{n} r_i x^i = r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1} + r_n x^n, \qquad \text{where } r_i \in R \text{ and } 0 \leq i \leq n.$$

The element p is usually denoted $p(x)$ to emphasize the *variable* x. Following the classical terminology, the r_i are called the *coefficients* of $p(x)$. Hence, we conclude that the elements of A have a polynomial writing, which justifies the name given to the ring.

DEFINITION 2.3 ([MR01, 1.2.8]). Let R be a ring and $A = R[x;\sigma,\delta]$ a skew polynomial ring over R. If $p(x) = \sum_{i=0}^{n} r_i x^i$ is an element of A such that $r_n \neq 0$, we define:

(i) $\deg(p(x)) := n$ as the *degree of* $p(x)$,

(ii) $\operatorname{lc}(p(x)) := r_n$ as the *leading coefficient*,

(iii) $\operatorname{lm}(p(x)) := x^n$ as the *leading monomial*,

(iv) $\operatorname{lt}(p(x)) := \operatorname{lc}(p(x))\operatorname{lm}(p(x)) = r_n x^n$ as the *leading term*.

If all coefficient of $p(x)$ are zero, we say that $p(x) := 0$ is the *zero polynomial* and in this case $\operatorname{lc}(0) := 0$, $\operatorname{lm}(0) := 0$ and $\operatorname{lt}(0) := 0$.

PROPOSITION 2.1 ([LEZ19C, REMARK 1.1.1]). *Let R be a ring and $A = R[x;\sigma,\delta]$ a skew polynomial ring over R. If $p(x), q(x) \in A$ and $p(x), q(x) \neq 0$, then*

(i) $\deg(p(x)) \geq 0$,

(ii) $\deg(p(x) + q(x)) \leq \max\{\deg(p(x)), \deg(q(x))\}$,

(iii) $\deg(p(x)q(x)) \leq \deg(p(x)) + \deg(q(x))$.

REMARK 17. Notice that no degree was defined for the zero polynomial. However, some authors put $\deg(0) := -\infty$, so (ii) and (iii) holds for every $p, q \in R[x;\sigma,\delta]$ (cf. [GW04, p. 37]).

Since our work concerns algebras, the next result establishes when an skew polynomial ring is an algebra induced by the base ring. We were not able to find a proof of such result in the literature.

LEMMA 2.2. *Let R be a K-algebra and $A = R[x;\sigma,\delta]$ a skew polynomial ring over R. A is a K-algebra having R as subalgebra if and only if σ is a K-linear map and $\delta(k1) = 0$, for every $k \in K$.*

Proof. ($\Rightarrow$) Suppose A is a K-algebra. Hence, for a given $k \in K$ we must have $(k1_R)x = x(k1_R)$, but by (O3) $x(k1_R) = \sigma(k1_R)x + \delta(k1_R)$. Comparing and using (O2) we get $\sigma(k1_R) = k1_R$ and $\delta(k1_R) = 0$.

($\Leftarrow$) Suppose σ is a K-linear map and $\delta(k1_R) = 0$ for every $k \in K$. We shall guarantee a ring morphism $\phi : K \to A$ such that $\operatorname{Im}(\phi) \subseteq Z(A)$. Since $1_A = 1_R$ and R is already a K-algebra, put

$$\phi(k) = k1_R, \qquad \text{for all } k \in K.$$

Obviously ϕ is an (unitary) ring morphism. Moreover by (O3), $x\phi(k) = \sigma(\phi(k))x + \delta(\phi(k)) = \sigma(k1_R)x + \delta(k1_R) = (k1_R)x = \phi(k)x$. Hence, $\operatorname{Im}(\phi) \subset Z(A)$. □

Throughout, every time we have the hypothesis that R is a K-algebra, we will automatically assume that σ and δ are such that A is also a K-algebra.

The next result states an universal property for skew polynomial rings.

THEOREM 2.3 (UNIVERSAL PROPERTY OF SKEW POLYNOMIAL RINGS, [GW04, PROPOSITION 2.4]). *Let R be a ring and $A = R[x;\sigma,\delta]$ a skew polynomial ring over R. Assume that B is a ring such that the following assertions hold:*

(i) *There is a ring morphism $\phi : R \to B$.*

(ii) *There is a distinguish element $y \in B$ such that $y\phi(r) = \phi(\sigma(r))y + \phi(\delta(r))$ for all $r \in R$.*

Then there is an uniquely ring morphism $\psi : R[x;\sigma,\delta] \to B$ such that $\psi(x) = y$ and $\psi|_R = \phi$. The last relation can be represented by the following commutative diagram:

$$\begin{array}{ccc} R & \xrightarrow{\ \iota\ } & R[x;\sigma,\delta] \\ {\scriptstyle\phi}\downarrow & \swarrow_{\psi} & \\ B & & \end{array} \tag{2.3}$$

Here $\iota : R \to R[x;\sigma,\delta]$ is the natural inclusion $\iota(r) := r$ for all $r \in R$. Moreover, if R and B are K-algebras and ϕ is a K-algebra morphism, then ψ is also a K-algebra morphism.

Proof. Notice that B has right R-module structure via $r \cdot b := \phi(r)b$, for all $r \in R$ and $b \in B$. On the other hand, by (O2), $R[x;\sigma,\delta]$ is a right free R-module with basis $\{x^i | i \geq 0\}$. Hence we can define a morphism of left R-modules $\psi : R[x;\sigma,\delta] \to B$ via $\psi(x^i) = y^i$, for all $i \geq 0$ (cf. [Lez19a, Theorem 7.3.1]). ψ is given by

$$\begin{aligned} \psi(r_0 + r_1x + \cdots + r_nx^n) &= r_0 \cdot \psi(1) + r_1 \cdot \psi(x) + \cdots r_n \cdot \psi(x^n) \\ &= \phi(r_0) + \phi(r_1)y + \cdots + \phi(r_n)y^n. \end{aligned}$$

By definition, (2.3) is commutative. Furthermore, ψ preserves the unity, since $\psi(1) = \psi(1x^0) = \phi(1)y^0 = 1$. We want ψ to be a ring morphism, so the only left to prove is that

$$\psi(rx^nsx^m) = \psi(rx^n)\psi(sx^m), \tag{2.4}$$

for all $r, s \in R$ and $n, m \in \mathbb{N}$. This is done by induction over n. The case $n = 0$ is trivial. If $n = 1$, we have

$$\begin{aligned} \psi(rxsx^m) &= \psi(r[\sigma(s)x + \delta(s)]x^m) = \psi(r\sigma(s)x^{m+1} + r\delta(s)x^m) = \psi(r\sigma(s)x^{m+1}) + \psi(r\delta(s)x^m) \\ &= \phi(r\sigma(s))y^{m+1} + \phi(r\delta(s))y^m = \phi(r)[\phi(\sigma(s))y + \phi(\delta(s))]y^m = \phi(r)y\phi(s)y^m \\ &= \psi(rx)\psi(sx^m). \end{aligned}$$

Assume that (2.4) holds for a fixed n. Then

$$\begin{aligned}\psi(rx^{n+1}sx^m) &= \psi(rx^nxsx^m) = \psi(rx^n[\sigma(s)x+\delta(s)]x^m) = \psi(rx^n\sigma(s)x^{m+1}) + \psi(rx^n\delta(s)x^m)\\ &= \psi(rx^n)\psi(\sigma(s)x^{m+1}) + \psi(rx^n)\psi(\delta(s)x^m) = \psi(rx^n)[\phi(\sigma(s))y+\phi(\delta(s))]y^m\\ &= \psi(rx^n)y\phi(s)y^m = \psi(rx^{n+1})\psi(sx^m).\end{aligned}$$

Therefore ψ is a ring morphism. By construction, ψ is uniquely determinated.

Now suppose that R, $R[x;\sigma,\delta]$ and B are K-algebras, and that ϕ is an algebra morphism. Then,

$$\psi(krx^i) = \phi(kr)y^i = k\phi(r)y^i = k\psi(rx^i),$$

for all $r \in R$, $k \in K$ and $i \geq 0$. This guarantees that ψ is K-linear and, since it is already a ring morphism, we have shown that it is an algebra morphism. □

COROLLARY 2.4 ([GW04, COROLLARY 2.5]). *Let R be a ring and $A = R[x;\sigma,\delta]$ a skew polynomial ring over R. If B is another ring such that*

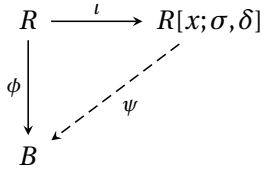
(i) *There is a ring morphism $\phi : R \to B$,*

(ii) *There is a distinguish element $y \in B$ such that $y\phi(r) = \phi(\sigma(r))y + \phi(\delta(r))$ for all $r \in R$,*

(iii) *B satisfies the universal property of Theorem 2.3.*

Then there exists a ring isomorphism between B and $R[x;\sigma,\delta]$.

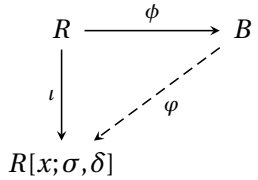
Proof. Since $R[x;\sigma,\delta]$ satisfies the universal property and the condition (ii) of Theorem 2.3 holds for B, there is an uniquely ring morphism $\phi : R[x;\sigma,\delta] \to B$ such that $\phi(x) = y$ and the diagram



is commutative. Similarly, since B satisfies the universal property and the relation

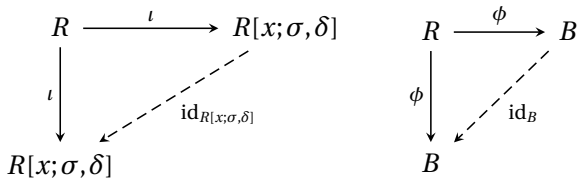
$$xr = \sigma(r)x + \delta(r) = \iota(\sigma(r))x + \iota(\delta(r)), \qquad \text{for all } r \in R,$$

holds in $R[x;\sigma,\delta]$, there exists an uniquely ring morphism $\varphi : B \to R[x;\sigma,\delta]$ such that $\varphi(y) = x$ and the diagram



is commutative. Moreover, using the respective universal properties of $R[x;\sigma,\delta]$ and B with

themselves, we get this two commutative diagrams:



Since $\varphi\psi(x) = x$ and $\varphi\psi\iota = \iota$, by uniqueness $\varphi\psi = \mathrm{id}_{R[x;\sigma,\delta]}$. Similarly, $\psi\varphi(y) = y$ and $\psi\varphi\phi = \phi$, so $\psi\varphi = \mathrm{id}_B$. Hence, we conclude $B \cong R[x;\sigma,\delta]$. □

A basic property of Ore extensions is the following.

PROPOSITION 2.5 ([LEZ19C, PROPOSITION 1.2.1]). *Let R be a ring and $A = R[x;\sigma,\delta]$ a skew polynomial ring over R such that σ is injective. If R is a domain, then A is also a domain.*

Proof. Let $p(x) = p_0 + p_1x + \cdots + p_nx^n \neq 0$ and $q(x) = q_0 + q_1x + \cdots + q_mx^m \neq 0$ be two elements of A such that $p_n, q_m \neq 0$. Then $\mathrm{lt}(pq) = p_n\sigma^n(q_m)x^{n+m} \neq 0$, by the injectivity if σ. Hence, $pq \neq 0$. □

Is immediate that, under these conditions, $\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$ for all $p, q \in A - \{0\}$. Moreover, $A^* = R^*$.

Recall that a ring R is said to be *left Noetherian* if any ascending chain of left ideals stabilizes (cf. [GW04, Propositicion 1.1]). We mention a theorem of huge relevance which generalizes the well known Hilbert's Basis Theorem for the commutative case; its complete proof can be found in [Lez19c, Theorem 1.2.6].

THEOREM 2.6 (HILBERT'S BASIS THEOREM FOR SKEW POLYNOMIAL RINGS, [GW04, THEOREM 2.6]). *Let R be a ring and $A = R[x;\sigma,\delta]$ a skew polynomial ring over R. If R is a left (resp. right) Noetherian ring and σ is bijective, then A is a left (resp. right) Noetherian ring.*

The construction of skew polynomial rings can be applied several times to obtain an *iterated skew polynomial ring* of the form $R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$. Notice that σ_i and δ_i must be defined as

$$\sigma_i, \delta_i : R[x_1;\sigma_1,\delta_1]\cdots[x_{i-1};\sigma_{i-1},\delta_{i-1}] \longrightarrow R[x_1;\sigma_1,\delta_1]\cdots[x_{i-1};\sigma_{i-1},\delta_{i-1}], \quad 1 \leq i \leq n.$$

For iterated skew polynomial rings an explicit basis over the original base ring is given.

LEMMA 2.7. *Let R be a ring and $A = R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$ an iterated skew polynomial ring over R. Then the set*

$$\mathrm{Mon}(x_1,\ldots,x_n) := \left\{x_1^{\alpha_1}\cdots x_n^{\alpha_n} : (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n\right\}$$

is a left R-basis of A.

Proof. Although this result is probably a well known fact, we were not able to find a proof of it in

the literature. We proceed for induction over n, the number of variables. We denote

$$A_i := R[x_1;\sigma_1,\delta_1]\cdots[x_i;\sigma_i,\delta_i], \qquad \text{for all } 1 \leq i \leq n.$$

Since for $n = 1$ the statement reduces to (O2), there is noting to prove.

Let $n = 2$. Then, again by (O2), the powers of x_2 form an left basis of $A = A_2$ over A_1, meaning that every element $p \in A_2$ can be written as

$$p = p_0(x_1) + p_1(x_1)x_2 + p_2(x_1)x_2^2 + \cdots + p_m(x_1)x_2^m,$$

with all $p_j(x_1) \in A_1$, $0 \leq j \leq m$. Since every $p_j(x_1)$ can be generated by powers of x_1, by distributivity, it is clear that p is generated by $\{x_1^{\alpha_1}x_2^{\alpha_2} : \alpha_1,\alpha_2 \in \mathbb{N}\}$. Now, suppose that

$$0 = \sum_{i,j=0}^{n,m} r_{ij}x_1^i x_2^j, \qquad \text{for some } r_{ij} \in R.$$

By associativity,

$$\sum_{i,j=0}^{n,m} r_{ij}x_1^i x_2^j = \sum_{j=0}^{m}\left(\sum_{i=0}^{n} r_{ij}x_1^i\right)x_2^j$$

so by linearly independence of the powers of x_2, $\sum_{i=0}^{n} r_{ij}x_1^i = 0$ for every $1 \leq j \leq m$. But, this time, by the linearly independence of the powers of x_1, every $r_{ij} = 0$.

Now, assume that $\mathrm{Mon}(x_1,\ldots,x_{n-1})$ is left basis for A_{n-1} over R. Similarly to the previous case, every $p \in A$ can be written as

$$p = p_0(x_1,\ldots,x_{n-1}) + p_1(x_1,\ldots,x_{n-1})x_n + p_2(x_1,\ldots,x_{n-1})x_{n-1}^2 + \cdots + p_m(x_1,\ldots,x_{n-1})x_{n-1}^m,$$

with all $p_j \in A_{n-1}$, $0 \leq j \leq m$. Using the induction hypothesis for every p_j, it is clear that $\mathrm{Mon}(x_1,\ldots,x_n)$ generates p. Now suppose that

$$0 = \sum_{\substack{0\leq\alpha_i\leq m_i\\ 1\leq i\leq n}} r_\alpha x_1^{\alpha_1}\cdots x_n^{\alpha_n}, \qquad \text{for some } r_\alpha \in R,\ \alpha := (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n.$$

Associating,

$$\sum_{\substack{0\leq\alpha_i\leq m_i\\ 1\leq i\leq n}} r_\alpha x_1^{\alpha_1}\cdots x_n^{\alpha_n} = \sum_{\alpha_n=0}^{n}\left(\sum_{\substack{0\leq\alpha_i\leq m_i\\ 1\leq i\leq n-1}} r_\alpha x_1^{\alpha_1}\cdots x_{n-1}^{\alpha_{n-1}}\right)x_n^{\alpha_n}.$$

Since the powers of x_n is a left basis for A over A_{n-1}, we must have

$$\sum_{\substack{0\leq\alpha_i\leq m_i\\ 1\leq i\leq n-1}} r_\alpha x_1^{\alpha_1}\cdots x_{n-1}^{\alpha_{n-1}} = 0,$$

but by induction hypothesis, that only happens if and only if every $r_\alpha = 0$, which shows the linearly independence of $\mathrm{Mon}(x_1,\ldots,x_n)$. □

Now, we review some examples. They evidence that skew polynomial rings are, indeed, a generalization of more particular and well known cases. They were adapted from [GW04], [Lez19c]

and [MR01]. Throughout the remaining of this section, let R be a ring, σ an endomorphism of R and δ a σ-derivation of R.

EXAMPLE 2.1 (CLASSICAL POLYNOMIAL RING). Take $\sigma = \mathrm{id}_R$ and $\delta = 0$. Therefore (O3) reduces to $xr = rx$, for all $r \in R$. This is simply the *classical univariate polynomial ring over* R, and we write $R[x; \mathrm{id}_R, 0] = R[x]$. Moreover the formula (2.2) corresponds to usual multiplication of monomials. Notice that in this case, Theorem 2.6 becomes the classical Hilbert's Basis Theorem.

More generally, we can consider the *classical multivariate polynomial ring over* R, $R[x_1, \ldots, x_n]$, as an Ore extension over R, where $\sigma_i = \mathrm{id}_R$ and $\delta_i = 0$, for all $1 \leq i \leq n$.

EXAMPLE 2.2 (POLYNOMIAL RING OF ENDOMORPHISM TYPE). Take $\delta = 0$. Then (O3) becomes $xr = \sigma(r)x$, for all $r \in R$. In this case we write $R[x; \sigma, 0] = R[x; \sigma]$. The formula (2.2) reduces to $(rx^n)(sx^m) = r\sigma^n(s)x^{n+m}$, for all $r, s \in R$ and $n, m \in \mathbb{N}$. A widely studied particular case is when σ is an automorphism of R.

EXAMPLE 2.3 (POLYNOMIAL RING OF DERIVATION TYPE). Take $\sigma = \mathrm{id}_R$. Then (O3) becomes $xr = rx + \delta(r)$, for all $r \in R$. In this case we write $R[x; id_A, \delta] = R[x; \delta]$. Moreover the formula (2.2) simplifies to

$$(rx^n)(sx^m) = r \sum_{k=0}^{n} \binom{n}{k} \delta^k(s) x^{n+m-k}, \qquad \text{for all } r, s \in R \text{ and } n, m \in \mathbb{N}.$$

The generalizations of Examples 2.2 and 2.3 to several variables (i.e., iterated skew polynomial rings) are straightforward and therefore omitted.

EXAMPLE 2.4 (ORE ALGEBRAS). Since the setup in general iterated skew polynomial rings can be cumbersome, usually some conditions are imposed:

$$\sigma_i(x_j) = x_j, \qquad j < i, \tag{2.5}$$
$$\delta_i(x_j) = 0, \qquad j < i, \tag{2.6}$$
$$\sigma_i\sigma_1 = \sigma_1\sigma_i, \qquad 1 \leq i \leq n, \tag{2.7}$$
$$\delta_i\delta_1 = \delta_1\delta_i, \qquad 1 \leq i \leq n, \tag{2.8}$$

where the two last relations are understood to be restricted to R. Although iterated skew polynomial rings satisfying these relations are common, we were not able to find in the literature a coined name for them. Notice that in the case of one single variable (i.e., no iteration) these relations trivialize.

It can be shown that (2.5)-(2.8) are equivalent to the following relations (cf. [Lez19c, Proposition 1.3.2]):

$$x_i x_j = x_j x_i, \qquad 1 \leq i, j \leq n, \tag{2.9}$$
$$\sigma_i(R), \delta_i(R) \subseteq R, \qquad 1 \leq i \leq n. \tag{2.10}$$

Therefore, under these conditions the maps σ_i, δ_i can be seen as $\sigma_i, \delta_i : R \to R$.

We mention a particular case of the above, distinguished by its well behavior on computational implementations (cf. [KJJ15]). Let $\Bbbk[t_1, \ldots, t_n]$ be a classical multivariate polynomial ring over $\Bbbk$. If $A = \Bbbk[t_1, \ldots, t_n][x_1; \sigma_n, \delta] \cdots [x_n; \sigma_n, \delta_n]$ is an iterated Ore extension satisfying

(2.5)-(2.8), then A is called an *Ore algebra*.

We present concrete cases of the above.

EXAMPLE 2.5 (ENVELOPING UNIVERSAL ALGEBRA OF $\mathfrak{sl}_2(\Bbbk)$). Recall from Example 1.9 that a $\Bbbk$-basis for $\mathfrak{sl}_2(\Bbbk)$ is formed by

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and thus $U := U(\mathfrak{sl}_2(\Bbbk))$ can be seen as a the $\Bbbk$-algebra generated by x, y, h attached to the relation $[x,y] = h$, $[h,x] = 2x$ and $[h,y] = -2y$. It is possible to show that U is isomorphic to either of the following iterated polynomial rings:

$$\Bbbk[x][h;\delta_1][y;\sigma_2,\delta_2] \cong \Bbbk[h][x;\sigma_1][y;\sigma_2,\delta_2],$$

where

$$\begin{aligned} \delta_1 &= 2x\frac{d}{dx}, & \sigma_1(h) &= h-2, & \sigma_2(x) &= x, \\ \sigma_2(h) &= h+2, & \delta_2(x) &= -h, & \delta_2(h) &= 0. \end{aligned}$$

Notice that, by Theorem 2.3 and Proposition 2.5, U is a Noetherian domain.

EXAMPLE 2.6 (QUANTUM ENVELOPING ALGEBRA OF $\mathfrak{sl}_2(\Bbbk)$). Recall from Example 1.11 that, for $q \in \Bbbk$ an invertible element such that $q \neq \pm 1$, $U_q := U_q(\mathfrak{sl}_2(\Bbbk))$ is the $\Bbbk$-algebra generated by e, f, k, k^{-1} attached to the relations

$$kk^{-1} = k^{-1}k = 1, \tag{2.11}$$

$$kek^{-1} = q^2 e, \tag{2.12}$$

$$kfk^{-1} = q^{-2} f, \tag{2.13}$$

$$[e,f] = ef - fe = \frac{k-k^{-1}}{q-q^{-1}}. \tag{2.14}$$

We saw there that this algebra is, in fact, a Hopf algebra. In this example we will show that it can also be seen as an iterated skew polynomial ring.

Let $A_0 := \Bbbk[k,k^{-1}]$ be the Laurent polynomial ring in the variable k, in which (2.11) is satisfied. Notice that A_0 is a Noetherian domain and that $\{k^l\}_{l\in\mathbb{Z}}$ is a $\Bbbk$-basis of A_0. Now, consider the automorphism σ_1 of A_0 given by $\sigma_1(k) := q^2 k$ and the respective Ore extension $A_1 := A_0[f;\sigma_1]$. Then, using a similar argument to the one given in the proof of Lemma 2.7, we can prove that a $\Bbbk$-basis for A_1 is $\{f^j k^l : j \in \mathbb{N}, l \in \mathbb{Z}\}$. Moreover, by Theorem 2.6, A_1 is a Noetherian domain. Notice that $fk = \sigma_1(k)f = q^2 kf$ which corresponds to the relation (2.13). By the universal property of free algebras and Theorem 2.3, A_1 is isomorphic to the free algebra generated by f, k, k^{-1} attached to the relations (2.11) and (2.13).

Now we construct $A_2 := A_1[e;\sigma_2,\delta]$. Let

$$\sigma_2(f^j k^l) := q^{-2l} f^j k^l, \qquad j \in \mathbb{N}, l \in \mathbb{Z}. \tag{2.15}$$

Then σ_2 is an automorphism of A_1. If we denote by $\delta(f)(k)$ the Laurent polynomial $\frac{k-k^{-1}}{q-q^{-1}}$, let

$$\delta(l^l) := 0, \qquad \delta(f^j k^l) := \sum_{i=0}^{j-1} f^{j-1}\delta(f)(q^{-2i}k)k^l. \tag{2.16}$$

We must verify that δ is a σ_2-derivation of A_1. For that, is sufficient to verify that, for every $j,m \in \mathbb{N}$ and $l,n \in \mathbb{Z}$,

$$\delta(f^j k^l f^m k^n) = \sigma_2(f^j k^l)\delta(f^m k^n) + \delta(f^j k^l) f^m k^n. \tag{2.17}$$

Indeed, starting from the right side of (2.17) and using (2.13), (2.15) and (2.16), we have

$$\begin{aligned}
&\sigma_2(f^j k^l)\delta(f^m k^n) + \delta(f^j k^l) f^m k^n \\
&= \sum_{i=0}^{m-1} q^{-2l} f^j k^l f^{m-1}\delta(f)(q^{-2i}k)k^n + \sum_{i=0}^{j-1} f^{j-1}\delta(f)(q^{-2i}k)k^l f^m k^n \\
&= \sum_{i=0}^{m-1} q^{-2l-2l(m-1)} f^{j+m-1}\delta(f)(q^{-2i}k)k^{l+n} + \sum_{i=0}^{j-1} q^{-2lm} f^{m+j-1}\delta(f)(q^{-2i-2m}k)k^{l+n} \\
&= \sum_{i=0}^{m-1} q^{-2lm} f^{m+j-1}\delta(f)(q^{-2i}k)k^{l+n} + \sum_{i=m}^{j+m-1} q^{-2lm} f^{m+j-1}\delta(f)(q^{-2i}k)k^{l+n} \\
&= q^{-2lm}\left(\sum_{i=0}^{j+m-1} f^{j+m-1}\delta(f)(q^{-2i}k)k^{l+n}\right) = q^{-2lm}\delta(f^{j+m}k^{l+n}) = \delta(f^j k^l f^m k^n).
\end{aligned}$$

Thus, in particular

$$\delta(f) = \frac{k-k^{-1}}{q-q^{-1}}, \qquad \text{and} \qquad \delta(k) = 0,$$

whence $ek = \sigma_2(k)e + \delta(k) = q^{-2}ke$, which corresponds to (2.12), and $ef = \sigma_2(f)e + \delta(f) = fe + \frac{k-k^{-1}}{q-q^{-1}}$, which is (2.14).

Therefore, U_q is isomorphic to the iterated skew polynomial ring $\Bbbk[k,k^{-1}][f;\sigma_1][e;\sigma_2,\delta]$ and thus, it is a Noetherian domain with $\Bbbk$-basis $\{e^i f^j k^l \,|\, i,j \in \mathbb{N}, l \in \mathbb{Z}\}$.

EXAMPLE 2.7 (THE ALGEBRA OF SHIFT OPERATORS). Let $\Bbbk[t]$ the classical univariate polynomial ring over a field $\Bbbk$. If $\sigma_h : \Bbbk[t] \to \Bbbk[t]$ is the endomorphism defined by $\sigma_h(p(t)) = p(t-h)$, for all $p(t) \in \Bbbk[t]$, then the skew polynomial ring $S_h = \Bbbk[t][x_h;\sigma_h]$ over $\Bbbk[t]$ is known as the *algebra of shift operators*. If $p(t), q(t) \in \Bbbk[t]$, the formula (2.2) becomes

$$p(t)x_h^n q(t)x_h^m = p(t)q(t-nh)x_h^{n+m}, \qquad \text{for all } n,m \in \mathbb{N}.$$

Notice that S_h is an Ore algebra; it is used to model time-delays systems if $\Bbbk = \mathbb{R}$ and $h > 0$ (cf. [CQR07]).

EXAMPLE 2.8 (WEYL ALGEBRA). Let $\Bbbk[t]$ be as in Example 2.7 and denote by $\frac{d}{dt}$ the derivate operator with respect to t. The skew polynomial ring $A_1(\Bbbk) = \Bbbk[t][x;\frac{d}{dt}]$ over $\Bbbk[t]$ is known as

the *first Weyl algebra*. If $p(t), q(t) \in \Bbbk[t]$ the formula (2.2) becomes

$$p(t)x^n q(t)x^m = p(t)\sum_{k=0}^{n}\binom{n}{k}q^{(k)}(t)x^{n+m-k}, \qquad \text{for all } m,n \in \mathbb{N}.$$

Here $q^{(k)}(t)$ is the k-th derivate of $q(t)$ with respect to t. More generally, the *n-th Weyl algebra* ($n \geq 1$) is defined as the Ore algebra $A_n(\Bbbk) := \Bbbk[t_1,\ldots,t_n][x_1;\frac{\partial}{\partial t_1}]\cdots[x_n;\frac{\partial}{\partial t_n}]$.

EXAMPLE 2.9 (THE MIXED ALGEBRA). For every $h \in \Bbbk$, we define the *mixed algebra* (also known as the *algebra of delayed differential operator*, cf. [CQR07]) as $D_h := \Bbbk[t][x;\frac{d}{dt}][x_h;\sigma_h]$, where σ_h is as in Example 2.7. Notice that $D_h = A_1(\Bbbk)[x_h;\delta_h]$ and hence it is an Ore algebra.

EXAMPLE 2.10 (THE ALGEBRA FOR MULTIDIMENSIONAL DISCRETE LINEAR SYSTEMS). The Ore algebra defined as $D := \Bbbk[t_1,\ldots,t_n][x_1;\sigma_1]\cdots[x_n;\sigma_n]$, where

$$\sigma_i(p(t_1,\ldots,t_n)) = p(t_1,\ldots,t_{i-1},t_i+1,t_{i+1},\ldots,t_n), \qquad \text{for } 1 \leq i \leq n,$$

is known as the *algebra for multidimensional discrete linear systems* (cf. [CQR07]).

2.2 PBW EXTENSIONS

Although skew polynomial rings describe a large amount of non-commutative algebras, they do not cover some remarkable examples, such as the generalized differential operator ring or the enveloping algebra of a finite dimensional Lie algebra. Hence, in [BG88] a new family of rings was define to cover algebras having the PBW property and polynomial aspect.

DEFINITION 2.4 (PBW EXTENSION, [BG88, §5]). Let R and A be two rings. We say that *A is a Poincaré-Birkhoff-Witt (PBW) extension of R*, if the following conditions hold:

(PBW1) A contains R as a proper subring,

(PBW2) (*PBW property*) There exist finitely many elements $x_1,\ldots,x_n \in A$ such that A is a free left R-module with basis

$$\mathrm{Mon}(A) := \left\{x_1^{\alpha_1}\cdots x_n^{\alpha_n} : \alpha := (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n\right\}.$$

(PBW3) For each $r \in R$ and every $1 \leq i \leq n$,

$$x_i r - r x_i \in R.$$

(PBW4) For every $1 \leq i,j \leq n$,

$$x_i x_j - x_j x_i \in R + Rx_1 + \cdots + Rx_n.$$

Under these conditions we will write $A = R\langle x_1,\ldots,x_n\rangle$, and R will be called the *ring of coefficients* of the extension.

The basis $\mathrm{Mon}(A)$ is usually called *the set of standard monomial* (of A) and also denoted by

$\text{Mon}(x_1,\dots,x_n)$. Inspired by the PBW Theorem (cf. Example 1.8), $\text{Mon}(A)$ is called a *PBW basis* for A. Notice that, in general, for $i \neq j$ the elements x_i and x_j do not commute.

REMARK 18. If only (PBW1) and (PBW2) hold, we say that A *is a ring of left polynomial type over* R with respect to $\{x_1,\dots,x_n\}$.

Before giving some properties, we review a few examples of PBW extensions, adapted from [Lez19c].

EXAMPLE 2.11 (ORE EXTENSIONS OF DERIVATION TYPE). Let R be a ring and let

$$A := R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$$

be an iterated Ore extension of R satisfying (2.5)-(2.8) (or equivalently, (2.9)-(2.10)). We say that A is *an (iterated) Ore extension of derivation type* if $\sigma_i = \text{id}_R$, for all $1 \leq i \leq n$. These extensions are all PBW extension, since, for every $r \in R$ and $1 \leq i, j \leq n$,

$$\begin{aligned} x_i r - r x_i &= \delta_i(r), \\ x_i x_j - x_j x_i &= 0, \end{aligned}$$

which proves (PBW3) and (PBW4). Condition (PBW1) is trivial from the definition of Ore extension and (PBW2) is Lemma 2.7. In particular, the classical multivariate polynomial ring (cf. Example 2.1) and Weyl algebras (cf. Example 2.8) are examples of PBW extensions.

Nevertheless, not every Ore extension is a PBW extension. Indeed, by taking $A = R[x;\sigma,\delta]$ with $\sigma \neq \text{id}_R$, condition (PBW3) does not hold. A particular example of this is the algebra of shift operators (cf. Example 2.7). The other inclusion is also not true, as the next example shows.

EXAMPLE 2.12 (UNIVERSAL ENVELOPING ALGEBRA OF A FINITE DIMENSIONAL LIE ALGEBRA). Let $\mathfrak{g}$ be a finite dimensional $\Bbbk$-Lie algebra with ordered basis $X = \{x_1,\dots,x_n\}$ and recall the PBW Theorem for the $\Bbbk$-algebra $U(\mathfrak{g})$ (cf. Example 1.8); this means that (PBW1) and (PBW2) are satisfied when $R = \Bbbk$. With this, it is immediate that $U(\mathfrak{g})$ is a PBW extension of $\Bbbk$, since for all $k \in \Bbbk$ and $x_i, x_j \in X$,

$$x_i k - k x_i = 0 \in \Bbbk \qquad \text{and} \qquad x_i x_j - x_j x_i = [x_i, x_j] \in \mathfrak{g} = \Bbbk x_i + \cdots + \Bbbk x_n \subseteq \Bbbk + \Bbbk x_i + \cdots + \Bbbk x_n,$$

which are precisely (PBW3) and (PBW4).

However, in general, $U(\mathfrak{g})$ is not necessarily an iterated skew polynomial ring (nor an Ore extension), since in the expansion of the product $x_i x_j$, variables x_k, with $k > j$, can appear. Nonetheless, for some particular Lie algebras, its enveloping algebra can be seen both as PBW extension and as iterated skew polynomial ring (cf. Example 2.5).

Finally, we give two more examples of PBW extensions involving the algebra $U(\mathfrak{g})$.

EXAMPLE 2.13 (TENSOR PRODUCT WITH THE UNIVERSAL ENVELOPING ALGEBRA OF A FINITE-DIMENSIONAL LIE ALGEBRA). Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra with basis $X = \{x_i\}_i$ and let R be an arbitrary $\Bbbk$-algebra. Notice that the $\Bbbk$-algebra $R \otimes U(\mathfrak{g})$ is also a left R-module via the multiplication by elements of R.

If $W := \{x_{i_1}^{\alpha_1}\cdots x_{i_t}^{\alpha_t} : x_{i_j} \in X,\ \alpha_i \geq 0,\ t \geq 1\}$ is the $\Bbbk$-basis for $U(\mathfrak{g})$ given by the PBW Theorem,

then $1 \otimes W := \{1 \otimes z : z \in W\}$ is an R-basis for $R \otimes U(\mathfrak{g})$. Indeed, if M is a left R-module given and $f : 1 \otimes W \to M$ is any function, then we can induce a $\Bbbk$-bilinear map $\overline{f} : R \times U(\mathfrak{g}) \to M$ given by

$$\left(r, \sum_i \lambda_i X_i\right) \mapsto r \cdot \sum_i \lambda_i f(1 \otimes X_i),$$

with $X_i \in W$ and $\lambda_i \in \Bbbk$. Hence, by the universal property of tensor products, we can uniquely induce a $\Bbbk$-linear map $f' : R \otimes U(\mathfrak{g}) \to M$ such that the diagram

$$\begin{array}{ccc} R \times U(\mathfrak{g}) & \xrightarrow{\iota} & R \otimes U(\mathfrak{g}) \\ {\scriptstyle \overline{f}}\downarrow & \swarrow_{f'} & \\ M & & \end{array}$$

is commutative, where ι is the canonical map. Notice that f' is, in fact, a R-morphism, since for every $s \in R$,

$$\begin{aligned} f'\left(s \cdot \left(r \otimes \sum_i \lambda_i X_i\right)\right) &= f'\left(sr \otimes \sum_i \lambda_i X_i\right) = \overline{f}\left(sr, \sum_i \lambda_i X_i\right) = (sr) \cdot \sum_i \lambda_i f(1 \otimes X_i) \\ &= s \cdot \left(r \cdot \sum_i \lambda_i f(1 \otimes X_i)\right) = s \cdot \overline{f}\left(r, \sum_i \lambda_i X_i\right) = s \cdot f'\left(r \otimes \sum_i \lambda_i X_i\right). \end{aligned}$$

Moreover, it is clear that the diagram

$$\begin{array}{ccc} 1 \otimes W & \xrightarrow{j} & R \otimes U(\mathfrak{g}) \\ {\scriptstyle f}\downarrow & \swarrow_{f'} & \\ M & & \end{array}$$

is commutative, where j is the inclusion map. Additionally, by the uniqueness of $\overline{f}$, f' is the only one satisfying such commutativity. Hence, since every function from $1 \otimes W$ to an arbitrary left module of R can be extended to a R-morphism from $R \otimes U(\mathfrak{g})$ to such module, $1 \otimes W$ is indeed an R-basis.

Notice that $R \hookrightarrow R \otimes U(\mathfrak{g})$ via $r \mapsto r \otimes 1 = r \cdot (1 \otimes 1)$, which corresponds to (PBW1). If $\mathfrak{g}$ is finite-dimensional with $X = \{x_1, \ldots, x_n\}$, then we just proved that

$$1 \otimes W = \{(1 \otimes x_1)^{\alpha_1} \cdots (1 \otimes x_n)^{\alpha_n} : \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\} = \mathrm{Mon}(1 \otimes x_1, \ldots, 1 \otimes x_n)$$

is an R-basis for $R \otimes U(\mathfrak{g})$, which is (PBW2). Furthermore, (PBW3) and (PBW4) hold, for if $r \in R$ and $1 \leq i, j \leq n$, then

$$\begin{gathered} (r \otimes 1)(1 \otimes x_i) - (1 \otimes x_i)(r \otimes 1) = r \otimes x_i - r \otimes x_i = 0 \in R, \\ (1 \otimes x_i)(1 \otimes x_j) - (1 \otimes x_j)(1 \otimes x_i) = 1 \otimes x_i x_j - x_j x_i = 1 \otimes [x_i, x_j] \in R + R(1 \otimes x_1) + \cdots + R(1 \otimes x_n). \end{gathered}$$

Thus $R \otimes U(\mathfrak{g})$ is a PBW extension of R.

EXAMPLE 2.14 (CROSSED PRODUCT WITH THE UNIVERSAL ENVELOPING ALGEBRA OF A FINITE-DIMENSIONAL LIE ALGEBRA). Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra with basis $X = \{x_i\}_i$ and let R be an arbitrary $\Bbbk$-algebra. Following [MR01, 1.7.12], we say that a $\Bbbk$-algebra S is a *crossed product* of R by $U(\mathfrak{g})$, if the following conditions hold:

(i) S contains R as a proper subalgebra,

(ii) There exists an injective $\Bbbk$-algebra morphism $\mathfrak{g} \to S$, denoted by $x \mapsto \overline{x}$,

(iii) $\overline{x}r - r\overline{x} \in R$ and $r \mapsto \overline{x}r - r\overline{x}$ is a $\Bbbk$-derivation of R, for all $r \in R$,

(iv) $\overline{x}\,\overline{y} - \overline{y}\,\overline{x} \in \overline{[x,y]} + R$, for all $x, y \in \mathfrak{g}$,

(v) S is a free right left R-module with the standard monomials over $\{\overline{x_i}\}$ as a basis.

In such case, we write $S = R * U(\mathfrak{g})$. According to the previous conditions, if X is finite (that is, $\mathfrak{g}$ is finite-dimensional), then $R * U(\mathfrak{g})$ is a PBW extension of R. Particular examples of crossed products with the universal enveloping algebra of a Lie algebra can be found in [MR01, 1.7.13].

2.3 SKEW PBW EXTENSIONS

We saw in the previous section that if the skew polynomial ring $A = R[x;\sigma,\delta]$ is such that $\sigma \neq \mathrm{id}_R$, then A is not a PBW algebra. In [GL11] a generalization of PBW algebras was introduced.

DEFINITION 2.5 (SKEW PBW EXTENSION, [GL11, DEFINITION 1]). Let R and A be two rings. We say that *A is a skew PBW extension of R*, if the following conditions hold:

(SPBW1) A contains R as a proper subring,

(SPBW2) There exist finitely many elements $x_1, \ldots, x_n \in A$ such that A is a free left R-module with basis

$$\mathrm{Mon}(A) := \mathrm{Mon}(x_1, \ldots, x_n) = \left\{ x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \right\}.$$

(SPBW3) For each $r \in R - \{0\}$ and every $1 \leq i \leq n$, there exists $c_{i,r} \in R - \{0\}$ such that

$$x_i r - c_{i,r} x_i \in R.$$

(SPBW4) For every $1 \leq i, j \leq n$, there exists $c_{i,j} \in R - \{0\}$ such that

$$x_i x_j - c_{i,j} x_j x_i \in R + Rx_1 + \cdots + Rx_n.$$

Under these conditions we will write $A = \sigma(R)\langle x_1, \ldots, x_n \rangle$, and R will be called the *ring of coefficients* of the extension.

REMARK 19. Several facts can be immediately deduced from Definition 2.5.

1. By (SPBW2), the elements $c_{i,r}$ and $c_{i,j}$ of (SPBW3) and (SPBW4) are unique.

2. For $i = j$, in (SPBW4), $c_{i,i} = 1$. Indeed, since $x_i^2 - c_{i,i}x_i^2 = 0$, then $1 - c_{i,i} = 0$. If $r = 0$, we define $c_{i,0} = 0$.

3. Every $c_{i,j} \in R$, with $1 \leq i < j \leq n$, is left invertible. Indeed, $c_{i,j}$ and $c_{j,i}$ are such that

$$x_i x_j - c_{i,j} x_j x_i \in R + Rx_1 + \cdots + Rx_n,$$
$$x_j x_i - c_{j,i} x_i x_j \in R + Rx_1 + \cdots + Rx_n.$$

   Since $\text{Mon}(A)$ is an R-basis then $1 = c_{i,j}c_{j,i}$.

4. We denote the elements of $\text{Mon}(A)$ as x^α when its important to highlight the exponents $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. An alternative notation for an arbitrary element of $\text{Mon}(A)$ is using the capital letter X. Notice that, by (SPBW2), each element $f \in A - \{0\}$ has a unique representation in the form $f = c_1X_1 + \ldots + c_tX_t$, with $c_i \in R - \{0\}$ and $X_i \in \text{Mon}(A)$, for every $1 \leq i \leq t$.

5. It is clear that the verification of (SPBW2) in most cases can be cumbersome. There are several techniques for that purpose, including Lemma 2.7 for skew polynomial rings, computation of Gröbner bases of two-sided ideals for free algebras (cf. [Lev05]), the Bergman's Diamond Lemma (cf. [Ber78, Rey13]) and the existence Theorem for PBW extensions (cf. [Aco14, AL15]).

The following result justifies the notation for skew PBW extensions.

PROPOSITION 2.8 ([GL11, PROPOSITION 3]). *Let A be a skew PBW extension of R. Then, for $1 \leq i \leq n$, there exist an injective ring endomorphism $\sigma_i : R \to R$ and a σ_i-derivation $\delta_i : R \to R$ such that*

$$x_i r = \sigma_i(r)x_i + \delta_i(r), \qquad \textit{for every } r \in R.$$

Proof. By (SPBW3), for every $1 \leq i \leq n$ and each $r \in R$, there exist elements $c_{i,r}, r_i \in R$ such that $x_i r = c_{i,r}x_i + r_i$. Since $\text{Mon}(A)$ is a R-basis of A, there elements are unique for r, so we can define the maps $\sigma_i, \delta_i : R \to R$ by $\sigma_i(r) := c_{i,r}$ and $\delta_i(r) := r_i$. Moreover, it is clear that, if $r \neq 0$, then $c_{i,r} \neq 0$ so σ_i is indeed injective. Is easy to check that σ_i is an endomorphism and that δ_i is a σ_i-derivation. □

A particular case for skew PBW extension is when all derivations d_i are zero. Another interesting situation is when all σ_i are bijective and the constants $c_{ij} \in R$ are invertible.

DEFINITION 2.6 (QUASI-COMMUTATIVE AND BIJECTIVE SKEW PBW EXTENSIONS, [GL11, DEFINITION 4]). Let A be a skew PBW extension of R.

(i) A is said to be *quasi-commutative* if (SPBW3) and (SPBW4) are replaced by

(SPBW3') For every $1 \leq i \leq n$ and $r \in R - \{0\}$, there exists $c_{i,r} \in R - \{0\}$ such that

$$x_i r = c_{i,r}x_i.$$

(SPBW4') For every $1 \leq i, j \leq n$, there exists $c_{i,j} \in R - \{0\}$ such that

$$x_j x_i = c_{i,j} x_i x_j.$$

(ii) A is said to be *bijective* if σ_i is bijective, for every $1 \leq i \leq n$, and each $c_{i,j}$ is invertible, for any $1 \leq i, j \leq n$.

Some examples of skew PBW extensions are the following. They are adapted from [Li02] and [GL11].

EXAMPLE 2.15 (PBW EXTENSIONS). any PBW extensions is a bijective skew PBW extension since, in this case, $\sigma_i = \mathrm{id}_R$ $(1 \leq i \leq n)$ and $c_{i,j} = 1$ $(1 \leq i, j \leq n)$.

EXAMPLE 2.16 (ORE EXTENSIONS OF INJECTIVE TYPE). Any Ore extension $A = R[x; \sigma, \delta]$ with σ injective is a skew PBW extension, $R[x; \sigma, \delta] = \sigma(R)\langle x \rangle$. If additionally $\delta = 0$, then $R[x; \sigma]$ is quasi-commutative.

Moreover, an iterated skew polynomial ring $A = R[x_1; \sigma_1, \delta_1] \cdots [x_n; \sigma_n, \delta_n]$ is a skew PBW extension of R, if the following conditions hold:

(i) σ_i is injective, for $1 \leq i \leq n$.

(ii) $\sigma_i(R), \delta_i(R) \subseteq R$, for $1 \leq i \leq n$.

(iii) There exist $c, d \in R$ such that c is left invertible and $\sigma_j(x_i) = c x_i + d$, for $i < j$.

(iv) $\delta_j(x_i) \in R + R x_1 + \cdots + R x_n$, for $i < j$.

Under these conditions we have $A = R[x_1; \sigma_1, \delta_1] \cdots [x_n; \sigma_n, \delta_n] = \sigma(R)\langle x_1, ..., x_n \rangle$ and A is called *of injective type*.

A particular case of such situation are iterated Ore extensions satisfying (2.5)-(2.8) with each σ_i is injective. If specifically $R = \mathbb{k}[t_1, \ldots, t_n]$, then we have an Ore algebra (cf. Example 2.4), and

$$\mathbb{k}[t_1, \ldots, t_n][x_1; \sigma_n, \delta] \cdots [x_n; \sigma_n, \delta_n] = \sigma(\mathbb{k}[t_1, \ldots, t_n])\langle x_1, \ldots, x_n \rangle.$$

Concrete examples are the algebra of shift operators S_h (cf. Example 2.7), the Weyl algebras $A_n(\mathbb{k})$ (cf. Example 2.8), the mixed algebra D_h (cf. Example 2.9) and the algebra for multidimensional discrete linear systems D (cf. Example 2.10). Observe that all of these examples are not PBW extensions.

EXAMPLE 2.17 (ADDITIVE ANALOGUE OF THE WEYL ALGEBRA). Given $q_1, \ldots, q_n \in \mathbb{k} - \{0\}$, let $A_n(q_1, \ldots, q_n)$ be the algebra generated by $x_1, \ldots, x_n, y_1, \ldots, y_n$ together with the relations

$$\begin{aligned} x_j x_i = x_i x_j, \qquad y_j y_i = y_i y_j, \qquad & \text{for } 1 \leq i, j \leq n, \\ y_i x_j = x_j y_i, \qquad & \text{for } i \neq j, \\ y_i x_i = q_i x_i y_i + 1, \qquad & \text{for } 1 \leq i \leq n. \end{aligned}$$

$A_n(q_1, \ldots, q_n)$ is known as the *additive analogue of the Weyl algebra* (introduced by [Kur80]) and is isomorphic to the iterated skew polynomial ring $\mathbb{k}[x_1, \ldots, x_n][y_1; \sigma_1, \delta_1] \cdots [y_n; \sigma_n, \delta_n]$ over

$\Bbbk[x_1,\dots,x_n]$, where

$$\begin{aligned} \sigma_j(y_i) = y_i, \qquad \delta_j(y_i) = 0, \qquad & \text{for } 1 \le i < j \le n, \\ \sigma_i(x_j) = x_j, \qquad \delta_i(x_j) = 0, \qquad & \text{for } i \ne j, \\ \sigma_i(x_i) = q_i x_i, \qquad \delta_i(x_i) = 1, \qquad & \text{for } 1 \le i \le n. \end{aligned}$$

Since $A_n(q_1,\dots,q_n)$ is an iterated Ore extension of injective type, it is also a skew PBW extension of $\Bbbk[x_1,\dots,x_n]$. Moreover, it is bijective and

$$A_n(q_1,\dots,q_n) = \sigma(\Bbbk[x_1,\dots,x_n])\langle y_1,\dots,y_n\rangle.$$

Nonetheless, notice that $A_n(q_1,\dots,q_n)$ can also be viewed as a skew PBW extension of $\Bbbk$, by putting

$$A_n(q_1,\dots,q_n) = \sigma(\Bbbk)\langle x_1,\dots,x_n,y_1,\dots,y_n\rangle.$$

If $q_i = q \ne 0$, for all $1 \le i \le n$, then $A_n(q_1,\dots,q_n)$ becomes the *algebra of q-differential operators* (cf. [JBSZ81]).

EXAMPLE 2.18 (MULTIPLICATIVE ANALOGUE OF THE WEYL ALGEBRA). Given $\lambda_{ji} \in \Bbbk - \{0\}$, with $1 \le i < j \le n$, let $\mathcal{O}_n(\lambda_{ij})$ be the algebra generated by $x_1,\dots,x_n$ and subject to the relations

$$x_j x_i = \lambda_{ji} x_i x_j, \qquad \text{for } 1 \le i < j \le n.$$

$\mathcal{O}_n(\lambda_{ij})$ is known as the *multiplicative analogue of the Weyl algebra* (introduced by [Jat84]) and is isomorphic to the iterated skew polynomial ring $\Bbbk[x_1][x_2;\sigma_2]\cdots[x_n;\sigma_n]$ over $\Bbbk[x_1]$, where

$$\sigma_j(x_i) = \lambda_{ji} x_i, \qquad \text{for } 1 \le i < j \le n.$$

Since $\mathcal{O}_n(\lambda_{ij})$ satisfies the conditions (i)-(iv) of Example 2.16, it is also a skew PBW extension of $K[x_1]$ and hence

$$\mathcal{O}_n(\lambda_{ij}) = \sigma(K[x_1])\langle x_2,\dots,x_n\rangle.$$

Notice that $\mathcal{O}_n(\lambda_{ij})$ is quasi-commutative and bijective, and can also be viewed as a skew PBW extension of $\Bbbk$ by putting

$$\mathcal{O}_n(\lambda_{ij}) = \sigma(\Bbbk)\langle x_1,\dots,x_n\rangle.$$

$\mathcal{O}_n(\lambda_{ij})$ is also called the *homogeneous solvable polynomial algebra*. If $n = 2$, then $\mathcal{O}_2(\lambda_{21})$ is the *quantum plane* (cf. [Man18]). If all $\lambda_{ji} = q^{-2} \ne 0$, for some $q \in \Bbbk - \{0\}$, then $\mathcal{O}_n(\lambda_{ij})$ becomes the well-known *coordinate ring of the the quantum affine n-space* (cf. [Smi92]).

EXAMPLE 2.19 (q-HEISENBERG ALGEBRA). Given $q \in \Bbbk - \{0\}$, let $h_n(q)$ be the algebra generated by $x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n$ together with the relations

$$\begin{aligned} x_j x_i = x_i x_j, \qquad z_j z_i = z_i z_j, \qquad y_j y_i = y_i y_j, \qquad & \text{for } 1 \le i,j \le n, \\ z_j y_i = y_i z_j, \qquad z_j x_i = x_i z_j, \qquad y_j x_i = x_i y_j, \qquad & \text{for } i \ne j, \\ z_i y_i = q y_i z_i, \qquad z_i x_i = q^{-1} x_i z_i + y_i, \qquad y_i x_i = q x_i y_i, \qquad & \text{for } 1 \le i \le n. \end{aligned}$$

$h_n(q)$ is known as the *q-Heisenberg algebra* (introduced by [Ber92]) and is isomorphic to the iter-

ated skew polynomial ring $\Bbbk[x_1,\dots,x_n][y_1;\sigma_1]\cdots[y_n;\sigma_n][z_1;\theta_1,\delta_1]\cdot[z_n;\theta_n,\delta_n]$ over $\Bbbk[x_1,\dots,x_n]$, where

$$\theta_j(z_i)=z_i,\qquad \delta_j(z_i)=0,\qquad \sigma_j(y_i)=y_i,\qquad \text{for } 1\leq i<j\leq n,$$
$$\theta_j(y_i)=y_i,\qquad \delta_j(y_i)=0,\qquad \theta_j(x_i)=x_i,\qquad \delta_j(x_i)=0,\qquad \sigma_j(x_i)=x_i,\qquad \text{for } i\neq j,$$
$$\theta_i(y_i)=qy_i,\qquad \delta_i(y_i)=0,\qquad \theta_i(x_i)=q^{-1}x_i,\qquad \delta_i(x_i)=y_i,\qquad \sigma_i(x_i)=qx_i,\qquad \text{for } 1\leq i\leq n.$$

Note that, since $\delta_i(x_i)=y_i\neq\Bbbk[x_1,\dots,x_n]$, considering the extension over $\Bbbk[x_1,\dots,x_n]$, $h_n(q)$ does not satisfies the condition (iii) of Example 2.16. However, if the base ring is $\Bbbk$, it does satisfies conditions (i)-(iv) and hence $h_n(q)$ is a bijective skew PBW extension of $\Bbbk$,

$$h_n(q)=\sigma(\Bbbk)\langle x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n\rangle.$$

This algebra has its roots in the study of q-calculus (cf. [Wal85]).

From these examples one could think that all skew PBW extensions are (iterated) skew polynomial rings of injective type. However, that is not the case as the following examples show.

EXAMPLE 2.20 (QUANTUM ALGEBRA $U_q'(\mathfrak{so}_3)$). Given $q\in\Bbbk-\{0\}$, let $U_q'(\mathfrak{so}_3)$ be the algebra generated by I_1,I_2,I_3 together with the relations

$$I_2I_1-qI_1I_2=-q^{1/2}I_3,\qquad I_3I_1-q^{-1}I_1I_3=q^{-1/2}I_2,\qquad I_3I_2-qI_2I_3=-q^{1/2}I_1.$$

In [Aco14] is shown in detail that this algebra is indeed a PBW extension of $\Bbbk$, i.e.,

$$U_q'(\mathfrak{so}_3)=\sigma(\Bbbk)\langle I_1,I_2,I_3\rangle.$$

Moreover, from the relations it is clear that it can not be expressed as a skew polynomial ring, since the commutation rule of two variables involves the third. This algebra was introduced in [GK91] and is a nonstandard q-deformation of the universal enveloping algebra $U(\mathfrak{so}_3)$ of the Lie algebra $\mathfrak{so}_3$ (cf. [HKP00]).

EXAMPLE 2.21 (DISPIN ALGEBRA). Let $U(\mathfrak{osp}(1,2))$ be the algebra generated by x,y,z together with the relation

$$yz-zy=z,\qquad zx+xz=y,\qquad xy-yx=x.$$

Then $U(\mathfrak{osp}(1,2))=\sigma(\Bbbk)\langle x_1,x_2,x_3\rangle$. Again, due to the relations, this algebra can not be seen as a skew polynomial ring. $U(\mathfrak{osp}(1,2))$ corresponds to the universal enveloping algebra of the Lie superalgebra $\mathfrak{osp}(1,2)$ (cf. [Ros95, C4.1]).

EXAMPLE 2.22 (HAYASHI ALGEBRA). Given $q\in\Bbbk-\{0\}$, let $W_q(J)$ be the algebra generated by $x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n$ together with the relations

$$x_jx_i=x_ix_j,\qquad z_jz_i=z_iz_j,\qquad y_jy_i=y_iy_j,\qquad \text{for } 1\leq i,j\leq n,$$
$$z_jy_i=y_iz_j,\qquad z_jx_i=x_iz_j,\qquad y_jx_i=x_iy_j,\qquad \text{for } i\neq j,$$
$$z_iy_i=qy_iz_i,\qquad y_ix_i=qx_iy_i,\qquad \text{for } 1\leq i\leq n,$$
$$(z_ix_i-qx_iz_i)y_i=1=y_i(z_ix_i-qx_iz_i),\qquad \text{for } 1\leq i\leq n.$$

$W_q(J)$ is known as the *Hayashi algebra* (introduced by [Hay90]). Notice that $W_q(J)$ is a skew PBW extension of the multivariate Laurent polynomial ring $\mathbb{k}[y_1^{\pm 1},\dots,y_n^{\pm 1}]$, since

$$x_i y_j^{-1} = y_j^{-1} x_i, \qquad z_i y_j^{-1} = y_j^{-1} z_i, \qquad y_j y_j^{-1} = y_j^{-1} y_j = 1, \qquad \text{for } 1 \leq i, j \leq n,$$
$$z_i x_i = q x_i z_i + y_i^{-1}, \qquad \text{for } 1 \leq i \leq n.$$

Hence $W_q(J) = \sigma(\mathbb{k}[y_1^{\pm 1},\dots,y_n^{\pm 1}])\langle x_1,\dots,x_n,y_1,\dots,y_n\rangle$.

We end mentioning two remarkable properties of skew PBW extensions.

By (SPBW4), for every $1 \leq i, j \leq n$, we know that there exist an unique finite set of constants $c_{i,j}, d_{i,j}, a_{ij}^k \in R - \{0\}$ such that

$$x_i x_j = c_{i,j} x_j x_i + a_{ij}^{(1)} x_1 + \cdots + a_{ij}^{(n)} x_n + d_{ij}.$$

Such constants, together with the coefficient ring R, the number of variables n, the injective endomorphism σ_k and the σ_k-derivations δ_k are known as the *parameters* of the extension.

THEOREM 2.9 (UNIVERSAL PROPERTY OF SKEW PBW EXTENSIONS, [AL15, THEOREM 3.1]). *Let $A = \sigma(R)\langle x_1,\dots,x_n\rangle$ be a skew PBW extension of R with corresponding parameters R, n, σ_k, δ_k, c_{ij}, d_{ij}, $a_{ij}^{(k)}$, for $1 \leq i, j \leq n$ and $1 \leq k \leq n$. Let B a ring with a ring morphism $\phi : R \to B$ and elements $y_1,\dots,y_n$ such that:*

(i) $y_k \phi(r) = \phi(\sigma_k(r)) y_k + \phi(\delta_k(r))$, *for every $r \in R$ and $1 \leq k \leq n$,*

(ii) $y_j y_i = \phi(c_{ij}) y_i y_j + \phi(a_{ij}^{(1)}) y_1 + \cdots + \phi(a_{ij}^{n}) y_n + \phi(d_{ij})$, *for every $1 \leq i, j \leq n$.*

Then, there exists an unique ring morphism $\psi : A \to B$ such that $\psi(x_i) = y_i$, for $1 \leq i \leq n$, and the following diagram

$$\begin{array}{ccc} R & \xrightarrow{\iota} & \sigma(R)\langle x_1,\dots,x_n\rangle \\ {\scriptstyle\phi}\downarrow & \swarrow_{\psi} & \\ B & & \end{array} \tag{2.18}$$

is commutative, where ι is the inclusion map.

THEOREM 2.10 (HILBERT'S BASIS THEOREM FOR SKEW PBW EXTENSIONS, [GL11, THEOREM 10]). *Let $A = \sigma(R)\langle x_1,\dots,x_n\rangle$ be a bijective skew PBW extension of R. If R is a left (resp. right) Noetherian ring then A is also a left (resp. right) Noetherian ring.*

The proof of this result uses techniques of graduation-filtration (cf. Appendix A), since the graded associated ring of A is always an iterated skew polynomial ring of endomorphism type.

Several other properties of skew PBW extensions regarding quantum algebras have been studied in [RS17a, RS17b, RS17c, RS17d, JR18, RS18a, RS18b].

Recently, a more general type of non-commutative rings called *semi-graded*, containing all skew PBW extensions, was defined in [LL17]. Their properties and some connections with non-commutative geometry have been studied in the seminar *Seminario de Álgebra Constructiva* (SAC^2), https://sites.google.com/a/unal.edu.co/sac2/.

2.4 ALMOST SYMMETRIC ALGEBRAS

In this section we introduce a certain class of $\mathbb{N}$-filtered algebras whose main purpose is to generalize universal enveloping algebras of Lie algebras. Several preliminaries of graded and filtered rings will be used (cf. Appendix A).

DEFINITION 2.7 (ALMOST SYMMETRIC ALGEBRA, [LOD98, 3.3.8]). Let A be a $\mathbb{N}$-filtered algebra over $\Bbbk$. A is said to be *almost symmetric*, if there exists a graded isomorphism between $\mathrm{gr}(A)$ and the symmetric algebra $S(\mathrm{gr}(A)_1)$.

REMARK 20. Notice that if A is an almost symmetric algebra, then $F_0(A) = \Bbbk$. Indeed, since $S(\mathrm{gr}(A)_1)$ is connected (cf. Example A.4) we have $\mathrm{gr}(A)_0 = \Bbbk$. But

$$\mathrm{gr}(A)_0 = F_0(A)/F_{-1}(A) = F_0(A)/0 \cong F_0(A) = \Bbbk.$$

In order to classify these algebras, we give some definitions. Recall that, for any $\Bbbk$-vector space V, a bilinear form $f : V \times V \to \Bbbk$ is said to be *alternating* if $f(v,v) = 0$, for all $v \in V$.

DEFINITION 2.8 (2-COCYCLES, [SRI61, §1]). Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $f : \mathfrak{g} \times \mathfrak{g} \to \Bbbk$ a bilinear alternating form. We say that f is a *2-cocycle* of $\mathfrak{g}$, if

$$f(x,[y,z]) + f(y,[z,x]) + f(z,[x,y]) = 0, \qquad \text{for all } x,y,z \in \mathfrak{g}.$$

The set of 2-cocycles of $\mathfrak{g}$ is denoted by $Z^2(\mathfrak{g},\Bbbk)$.

DEFINITION 2.9 (SRIDHARAN ENVELOPING ALGEBRA, [SRI61, DEFINITION 2.1]). Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $f \in Z^2(\mathfrak{g},\Bbbk)$. If $T(\mathfrak{g})$ is the tensor algebra over $\mathfrak{g}$ and

$$I_f := \langle x \otimes y - y \otimes x - [x,y] - f(x,y) : x,y \in \mathfrak{g} \rangle,$$

the (associative) algebra $U_f(\mathfrak{g}) := T(\mathfrak{g})/I_f$ is called a *f-Sridharan enveloping algebra* of $\mathfrak{g}$.

LEMMA 2.11. *Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $f \in Z^2(\mathfrak{g},\Bbbk)$. Then $U_f(\mathfrak{g})$ is $\mathbb{N}$-filtered.*

Proof. Since $T(\mathfrak{g})$ is $\mathbb{N}$-graded (cf. Example A.3), the family $\{\bigoplus_{i\leq p}\mathfrak{g}^{\otimes i}\}_{p\in\mathbb{N}}$ is a $\mathbb{N}$-filtration. Hence, by Proposition A.2, the quotient $U_f(\mathfrak{g}) = T(\mathfrak{g})/I_f$ is also $\mathbb{N}$-filtered. Explicitly,

$$F_p(U_f(\mathfrak{g})) := \eta_f\left(\bigoplus_{i\leq p}\mathfrak{g}^{\otimes i}\right), \qquad \text{for all } p \in \mathbb{N},$$

where $\eta_f : T(\mathfrak{g}) \to U_f(\mathfrak{g}) = T(\mathfrak{g})/I_f$ is the canonical map, i.e., $\eta_f(z) = \overline{z} := z + I_f$, for every $z \in T(\mathfrak{g})$. □

The restriction of $\eta_f : T(\mathfrak{g}) \to U_f(\mathfrak{g})$ to $\mathfrak{g}$ induces a $\Bbbk$-linear map $i_f : \mathfrak{g} \to U_f(\mathfrak{g})$ which, for

every $x, y \in \mathfrak{g}$, satisfies

$$\begin{aligned} i_f(x)i_f(y) - i_f(y)i_f(x) &= \overline{xy} - \overline{yx} = \overline{x \otimes y - y \otimes x} \\ &= \overline{[x,y] + f(x,y)} = i_f([x,y]) + f(x,y) \cdot i_f(1). \end{aligned} \tag{2.19}$$

LEMMA 2.12 ([SRI61, LEMMA 2.4]). *Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $f \in Z^2(\mathfrak{g}, \Bbbk)$. Given $x_1, \ldots, x_p \in \mathfrak{g}$ and a permutation σ of $(1, \ldots, p)$, we have*

$$i_f(x_1) \cdots i_f(x_p) - i_f(x_{\sigma(1)}) \cdots i_f(x_{\sigma(p)}) \in F_{p-1}(U_f(\mathfrak{g})).$$

Proof. Decomposing the permutation as a product of transpositions, it is sufficient to consider the case of a transposition interchanging two consecutive indexes j and $j+1$. In this case, the relation (2.19) gives

$$i_f(x_j)i_f(x_{j+1}) - i_f(x_{j+1})i_f(x_j) = i_f([x_j, x_{j+1}]) + f(x_j, x_{j+1}) \cdot i_f(1).$$

Since $[x_j, x_{j+1}] \in \mathfrak{g}$ and $f(x_j, x_{j+1}) \in \Bbbk$, we have $i_f([x_j, x_{j+1}]) + f(x_j, x_{j+1}) \cdot i_f(1) \in F_2(U_f(\mathfrak{g}))$, as required. □

PROPOSITION 2.13 ([SRI61, PROPOSITION 2.3]). *Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $f \in Z^2(\mathfrak{g}, \Bbbk)$. Then $\operatorname{gr}(U_f(\mathfrak{g}))$ is a commutative algebra.*

Proof. Notice that the set $\{i_f(x) : x \in \mathfrak{g}\} \cup \{i_f(1)\}$ generates $U_f(\mathfrak{g})$ as an algebra. By Lemma 2.12 those generators commute in the associated graded algebra $\operatorname{gr}(U_f(\mathfrak{g}))$ and hence it must be commutative. □

Let $X = \{x_i\}_{i \in J}$ be a $\Bbbk$-basis for $\mathfrak{g}$ and $\leq$ a total order in J. In [Sri61, Theorem 2.6] is shown that the set containing 1 and all *standard monomials* of the form

$$i_f(x_{i_1})i_f(x_{i_2}) \cdots i_f(x_{i_n}), \qquad \text{with } i_1 \leq i_2 \leq \cdots \leq i_n,$$

is a $\Bbbk$-basis of $U_f(\mathfrak{g})$. In other words, the PBW Theorem for Sridharan enveloping algebras holds. This is used to prove that i_f is injective (cf. [Sri61, Corollary 2.8]) and the following result.

THEOREM 2.14 ([SRI61, THEOREM 2.5]). *Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $f \in Z^2(\mathfrak{g}, \Bbbk)$. Then*

$$\operatorname{gr}(U_f(\mathfrak{g})) \cong S(\mathfrak{g}),$$

as graded algebras.

Recall that, for any Lie algebra $\mathfrak{g}$, a $\Bbbk$-subspace $\mathfrak{I}$ is said to be a *Lie ideal* if

$$[\mathfrak{I}, \mathfrak{g}] := \operatorname{span}_{\Bbbk}\{[x,y] : x \in \mathfrak{I}, y \in \mathfrak{g}\} \subseteq \mathfrak{I}.$$

In this case, the quotient space $\mathfrak{g}/\mathfrak{I}$ has Lie algebra structure given by

$$[\overline{x}, \overline{y}] := \overline{[x,y]}, \qquad \text{for all } x, y \in \mathfrak{g}.$$

The next result gives a complete characterization of almost symmetric algebras.

THEOREM 2.15 (SRIDHARAN'S CLASSIFICATION, [SRI61, §3]). *Let A be an almost symmetric algebra. Then there exist a Lie algebra $\mathfrak{g}$ and a 2-cocycle $f : \mathfrak{g} \otimes \mathfrak{g} \to \Bbbk$ such that $A \cong U_f(\mathfrak{g})$, as $\mathbb{N}$-filtered algebras.*

Proof. Since $\operatorname{gr}(A)$ is isomorphic to a symmetric algebra, it must be commutative and hence, for every $x, y \in F_1(A)$, we have $\overline{xy - yx} = \overline{0}$ in $\operatorname{gr}(A)_2 = F_2(A)/F_1(A)$. Thus $xy - yx \in F_1(A)$ and the $\Bbbk$-space $F_1(A)$ acquires a structure of Lie algebra given by

$$[x, y] := xy - yx, \qquad \text{for all } x, y \in F_1(A).$$

Notice that $F_0(A) = \Bbbk$ is a Lie ideal of $F_1(A)$. Indeed, $[k, x] = kx - xk = 0$, for all $k \in \Bbbk$ and $x \in F_1(x)$. Hence $\mathfrak{g} := F_1(A)/\Bbbk$ has an induced Lie structure, given by

$$[\overline{x}, \overline{y}] = \overline{[x, y]} = \overline{xy - yx} = \overline{0}, \qquad \text{for all } x, y \in F_1(A).$$

In other words, $\mathfrak{g}$ is abelian. We have the exact short sequence

$$0 \longrightarrow \Bbbk \xrightarrow{\iota} F_1(A) \xrightarrow{j} \mathfrak{g} \longrightarrow 0,$$

where ι is the inclusion and j is the quotient map. Since this sequence is made of $\Bbbk$-vector spaces, it splits and hence there exist a $\Bbbk$-linear map $t : \mathfrak{g} \to F_1(A)$ such that $jt = \mathrm{id}_{\mathfrak{g}}$. Define the $\Bbbk$-bilinear map $f : \mathfrak{g} \times \mathfrak{g} \to \Bbbk$ by

$$f(\overline{x}, \overline{y}) := [t(x), t(y)] - t([x, y]), \qquad \text{for all } x, y \in F_1(A).$$

A quick computation shows that f is, in fact, a 2-cocycle, and then we can consider $U_f(\mathfrak{g})$. But by definition, $\operatorname{gr}(A) \cong S(\mathfrak{g})$. Hence, applying Theorem 2.14, we have $\operatorname{gr}(U_f(\mathfrak{g})) \cong S(\mathfrak{g})$, and by Proposition A.6, we get that $A \cong U_f(\mathfrak{g})$. □

This classification is used to endow any almost symmetric algebra with a comodule structure and obtain a new example of Hopf Galois extension.

THEOREM 2.16 ([JŞ06, PROPOSITION 6.4]). *Let A be an almost symmetric $\Bbbk$-algebra. Then there exists a Lie algebra $\mathfrak{g}$ such that A is an $U(\mathfrak{g})$-Galois object.*

Proof. By Theorem 2.15, there exist a Lie algebra $\mathfrak{g}$ and $f \in Z^2(\mathfrak{g}, \Bbbk)$ such that $A \cong U_f(\mathfrak{g})$. Let $h : T(\mathfrak{g}) \to U_f(\mathfrak{g}) \otimes U(\mathfrak{g})$ be the $\Bbbk$-linear map induced by

$$x \mapsto \overline{x} \otimes 1 + \overline{1} \otimes x, \qquad \text{for all } x \in \mathfrak{g}.$$

This map factorizes through an algebra map $\rho : U_f(\mathfrak{g}) \to U_f(\mathfrak{g}) \otimes U(\mathfrak{g})$ and hence $U_f(\mathfrak{g})$ is a $U(\mathfrak{g})$-comodule algebra such that

$$\rho(\overline{x}) = \overline{x} \otimes 1 + \overline{1} \otimes x, \qquad \text{for all } x \in \mathfrak{g}.$$

Let $X = \{x_i\}_{i \in J}$ be a $\Bbbk$-basis for $\mathfrak{g}$ and $\leq$ a total order in J. By the PBW Theorem there exists an

unique $\Bbbk$-linear map $\theta : U(\mathfrak{g}) \to U_f(\mathfrak{g})$ such that $\theta(1) = 1$ and

$$\theta(x_{i_1} x_{i_2} \cdots x_{i_n}) = \overline{x_{i_1}}\,\overline{x_{i_2}} \cdots \overline{x_{i_n}}, \qquad \text{for every } i_1 \leq i_2 \leq \cdots \leq i_n.$$

A straightforward computation shows that θ is in fact a $U(\mathfrak{g})$-comodule morphism. Moreover, θ is bijective and hence $U_f(\mathfrak{g})^{coU(\mathfrak{g})} = \Bbbk$. Then, by [Bel00, Proposition 1.5], it follows that $\Bbbk \subset U_f(\mathfrak{g})$ is an $U(\mathfrak{g})$-Galois object. □

[Bel00, Proposition 1.5] basically states that all faithfully flat $U(\mathfrak{g})$-Galois extensions $A^{coH} \subset A$ are characterized by maps $\lambda : \mathfrak{g} \to A$ such that $\rho(\lambda(x)) = \lambda(x) \otimes 1 + 1 \otimes x$, for all $x \in \mathfrak{g}$. In our case, such λ is what in the previous proof we called h.

We end this section mentioning a classification for Sridharan enveloping algebras (and thus for almost symmetric algebras) when the associated Lie algebra is of dimension three.

THEOREM 2.17 ([NUS91, THEOREM 1.3]). *Let $\mathfrak{g}$ be a $\Bbbk$-Lie algebra and $f \in Z^2(\mathfrak{g}, \Bbbk)$ such that $\dim_{\Bbbk}(\mathfrak{g}) = 3$. Then the Sridharan enveloping algebra $U_f(\mathfrak{g})$ is isomorphic to one of the ten following $\Bbbk$-algebras generated by x, y and z, together with the relations given.*

Type	$[x, y]$	$[y, z]$	$[z, x]$
1	0	0	0
2	0	x	0
3	x	0	0
4	0	αy	$-x$
5	0	$-y$	$-(x+y)$
6	z	$-2y$	$-2x$
7	1	0	0
8	1	x	0
9	x	1	0
10	1	y	x

Although some of these almost symmetric algebras are iterated skew polynomial rings (e.g. type 1, 7 or 8), not all of them are (e.g., type 6). Nevertheless, they all are skew PBW extensions and hence $U_f(\mathfrak{g}) \cong \sigma(\Bbbk)\langle x, y, z\rangle$.

CHAPTER 3

SOME INTERACTIONS

In this last part, we will review some relations between Hopf Galois extensions defined in Chapter 1 and some families and examples discussed in Chapter 2. Particularly, in Section 3.1 we describe coactions over skew polynomial rings. Section 3.2 relates almost symmetric algebras with Hopf Galois systems and Section 3.3 endows Kashiwara algebras with a quantum torsor structure. Throughout this chapter, H will denote an arbitrary K-Hopf algebra (faithfully flat, if needed). We follow the notation of Remark 15.

3.1 COACTIONS OVER SKEW POLYNOMIAL RINGS

We want to describe coactions of an arbitrary Hopf algebra H over a skew polynomial ring induced by the algebra of coefficients. For that, we develop some preliminary facts. The results of this section are all probably new.

LEMMA 3.1. *Let R, B be two K-algebras. If $A = R[x;\sigma,\delta]$ is a skew polynomial ring over R, then*

$$A \otimes_K B \cong (R \otimes_K B)[z;\sigma \otimes \mathrm{id}_B, \delta \otimes \mathrm{id}_B],$$
$$B \otimes_K A \cong (B \otimes_K R)[z;\mathrm{id}_B \otimes \sigma, \mathrm{id}_B \otimes \delta]$$

as K-algebras.

Proof. We shall prove the first isomorphism since the argument for the second one is quite similar. Notice that, since σ is a K-algebra morphism, $\sigma \otimes \mathrm{id}_B$ is also of the same type. Analogously, since δ is additive and $\delta(k1) = 0$, for all $k \in K$, it follows that $\delta \otimes \mathrm{id}_B$ is also additive and $(\delta \otimes \mathrm{id}_B)(k1 \otimes 1) = 0$. Furthermore, for all $r, s \in R$ and $b, c \in B$, we have

$$\begin{aligned}(\delta \otimes \mathrm{id}_B)[(r \otimes b)(s \otimes c)] &= (\delta \otimes \mathrm{id}_B)(rs \otimes bc) = \delta(rs) \otimes bc = (\sigma(r)\delta(s) + \delta(r)s) \otimes bc \\ &= \sigma(r)\delta(s) \otimes bc + \delta(r)s \otimes bc = (\sigma(r) \otimes b)(\delta(s) \otimes c) + (\delta(r) \otimes b)(s \otimes c) \\ &= [(\delta \otimes \mathrm{id}_B)(r \otimes b)][(\delta \otimes \mathrm{id}_B)(s \otimes c)] + [(\delta \otimes \mathrm{id}_B)(r \otimes b)](s \otimes c).\end{aligned}$$

Thus, $\delta \otimes \mathrm{id}_B$ is a $\sigma\,\mathrm{id}_B$-derivation of $R \otimes B$. Hence, the K-algebra $(R \otimes_K B)[z; \sigma \otimes \mathrm{id}_B, \delta \otimes \mathrm{id}_B]$ actually makes sense.

Now, since the map $R \times B \to A \otimes B$ given by $(r, b) \mapsto r \otimes b$ is K-bilinear, by the universal property of the tensor product, there exists a K-linear map $\phi : R \otimes B \to A \otimes B$ given by

$$\phi(r \otimes b) = r \otimes b, \qquad \text{for all} r \in R \subset A \text{ and } b \in B.$$

Notice that, in fact, ϕ is a K-algebra morphism. Since for all $r \in R$,

$$\begin{aligned}(x \otimes 1)\phi(r \otimes b) &= (x \otimes 1)(r \otimes b) = xr \otimes b = (\sigma(r)x + \delta(r)) \otimes b \\ &= \sigma(r)x \otimes b + \delta(r) \otimes b = \phi(\sigma(r) \otimes b)(x \otimes 1) + \sigma(\delta(b) \otimes b) \\ &= \phi[(\sigma \otimes \mathrm{id}_B)(r \otimes b)](x \otimes 1) + \phi[(\delta \otimes \mathrm{id}_B)(r \otimes b)],\end{aligned}$$

by Theorem 2.3, there exists an uniquely K-algebra morphism

$$\psi : (R \otimes B)[z; \sigma \otimes \mathrm{id}_B, \delta \otimes \mathrm{id}_B] \to A \otimes B$$

such that $\psi(z) = x \otimes 1$ and $\phi|_{R \otimes B} = \phi$. Explicitly, ψ is given by

$$\psi\left(\sum_{i=0}^{n} (r_i \otimes b_i) z^i\right) = \sum_{i=0}^{n} \phi(r_i \otimes b_i)(x \otimes 1)^i = \sum_{i=0}^{n} (r_i \otimes b_i)(x \otimes 1)^i = \sum_{i=0}^{n} r_i x^i \otimes b_i.$$

Conversely, since the map $A \times B \to (R \otimes B)z; \sigma \otimes \mathrm{id}_B, \delta \otimes \mathrm{id}_B]$ given by

$$\left(\sum_{i=0}^{n} r_i x^i, b\right) \mapsto \sum_{i=0}^{n} (r_i \otimes b) z^i$$

is K-bilinear, by the universal property of the tensor product, there exists a K-linear map $\varphi : A \otimes B \to (R \otimes B)[z; \sigma \otimes \mathrm{id}_B, \delta \otimes \mathrm{id}_B]$ given by

$$\varphi\left(\sum_{i=0}^{n} r_i x^i \otimes b\right) = \sum_{i=0}^{n} (r_i \otimes b) z^i.$$

Now, since

$$\begin{aligned}\psi\varphi\left(\sum_{i=0}^{n} r_i x^i \otimes b\right) &= \psi\left(\sum_{i=0}^{n} (r_i \otimes b) z^i\right) = \sum_{i=0}^{n} r_i x^i \otimes b, \\ \varphi\psi\left(\sum_{i=0}^{n} (r_i \otimes b_i) z^i\right) &= \varphi\left(\sum_{i=0}^{n} r_i x^i \otimes b_i\right) = \sum_{i=0}^{n} \varphi(r_i x^i \otimes b_i) = \sum_{i=0}^{n} (r_i \otimes b_i) z^i,\end{aligned}$$

the isomorphism holds. □

Via the isomorphism, the indeterminate z in $(R \otimes B)[z; \sigma \otimes \mathrm{id}_B, \delta \otimes \mathrm{id}_B]$ can be identify with the element $x \otimes 1$ of $R[x; \sigma, \delta] \otimes B$, and hence we shall write $(R \otimes B)[x \otimes 1; \sigma \otimes \mathrm{id}_B, \delta \otimes \mathrm{id}_B]$.

PROPOSITION 3.2. *Let H be a K-Hopf algebra. Suppose that R is a right H-comodule algebra with structure map $\rho_R : R \to R \otimes H$, and let $A = R[x; \sigma, \delta]$ be a skew polynomial ring over R such that*

σ and δ are H-comodule morphisms. Then A is also a right H-comodule algebra with induced structure map $\rho_A : A \to A \otimes H$ given by

$$\rho_A\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes (r_i)_{(1)}, \qquad \text{with } r_i \in R,\ 0 \le i \le n.$$

Moreover, $A^{coH} = R^{coH}[x;\sigma,\delta]$, where σ and δ are considered restricted to R^{coH}.

Proof. By Lemma 3.1 we have $A \otimes H \cong (R \otimes H)[x \otimes 1; \sigma \otimes \mathrm{id}_H, \delta \otimes \mathrm{id}_H]$ as algebras. Hence, since R is a right comodule algebra, $\rho_R : R \to R \otimes H \subset (R \otimes H)[x \otimes 1; \sigma \otimes \mathrm{id}_H, \delta \otimes \mathrm{id}_H]$ is an algebra morphism (cf. Proposition 1.8). Moreover, for every $r \in R$, since σ and δ are comodule morphisms, we have

$$\begin{aligned}
\rho_R(\sigma(r))(x \otimes 1) + \rho_R(\delta(r)) &= (\sigma(r)_{(0)} \otimes \sigma(r)_{(1)})(x \otimes 1) + (\delta(r)_{(0)} \otimes \delta(r)_{(1)} \\
&= (\sigma(r_{(0)}) \otimes r_{(1)})(x \otimes 1) + (\delta(r_{(0)}) \otimes r_{(1)}) \\
&= [(\sigma \otimes \mathrm{id}_H)(r_{(0)} \otimes r_{(1)})](x \otimes 1) + (\delta \otimes \mathrm{id}_H)(r_{(0)} \otimes r_{(1)}) \\
&= (x \otimes 1)(r_{(0)} \otimes r_{(1)}) = (x \otimes 1)\rho_R(r).
\end{aligned}$$

Hence, by Theorem 2.3, there exists an algebra morphism

$$\overline{\rho} : A \to (R \otimes H)[x \otimes 1; \sigma \otimes \mathrm{id}_H, \delta \otimes \mathrm{id}_H]$$

such that $\overline{\rho}(x) = x \otimes 1$ and $\overline{\rho}|_R = \rho_R$. Explicitly,

$$\overline{\rho}\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=0}^{n} \rho_R(r_i)(x \otimes 1)^i = \sum_{i=0}^{n} ((r_i)_{(0)} \otimes (r_i)_{(1)})(x \otimes 1)^i.$$

Now, we use the isomorphism ψ of the proof of Lemma 3.1 to define the algebra morphism $\rho_A : A \to A \otimes H$ as $\rho_A := \psi\overline{\rho}$. Then, we have

$$\rho_A\left(\sum_{i=0}^{n} r_i x^i\right) = \psi\overline{\rho}\left(\sum_{i=0}^{n} r_i x^i\right) = \psi\left(\sum_{i=0}^{n} ((r_i)_{(0)} \otimes (r_i)_{(1)})(x \otimes 1)^i\right) = \sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes (r_i)_{(1)}.$$

Furthermore,

$$\begin{aligned}
[(\mathrm{id}_A \otimes \Delta)\rho_A]\left(\sum_{i=0}^{n} r_i x^i\right) &= (\mathrm{id}_A \otimes \Delta)\left(\sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes (r_i)_{(1)}\right) = \sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes (r_i)_{(1)} \otimes (r_i)_{(2)} \\
&= (\rho_A \otimes \mathrm{id}_H)\left(\sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes (r_i)_{(1)}\right) = [(\rho_A \otimes \mathrm{id}_H)\rho_A]\left(\sum_{i=0}^{n} r_i x^i\right), \\
[(\mathrm{id}_A \otimes \varepsilon)\rho_A]\left(\sum_{i=0}^{n} r_i x^i\right) &= (\mathrm{id}_A \otimes \varepsilon)\left(\sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes (r_i)_{(1)}\right) = \sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes \varepsilon((r_i)_{(1)})1 \\
&= \sum_{i=0}^{n} (r_i)_{(0)} \varepsilon((r_i)_{(1)}) x^i \otimes 1 = \sum_{i=0}^{n} r_i x^i \otimes 1,
\end{aligned}$$

which proves that A is a right H-comodule with structure map ρ_A. Moreover, since, ρ_A is an algebra morphism, by Proposition 1.8, A is a right H-comodule algebra.

Now, we define

$$R^{coH}[x;\sigma,\delta] := \left\{ \sum_{i=0}^{n} r_i x^i \in A : r_i \in R^{coH},\, 0 \le i \le n \right\} \subset A,$$

which, since σ and δ are comodule morphisms, is indeed a subalgebra of A. If $p(x) = \sum_{i=0}^{n} r_i x^i \in R^{coH}[x;\sigma,\delta]$, then

$$\rho_A(p(x)) = \rho_A\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=0}^{n} r_i x^i \otimes 1 = p(x) \otimes 1,$$

so $p(x) \in A^{coH}$. Conversely, if $p(x) = \sum_{i=0}^{n} r_i x^i \in A^{coH}$, then

$$\sum_{i=0}^{n} (r_i)_{(0)} x^i \otimes (r_i)_{(1)} = \sum_{i=0}^{n} r_i x^i \otimes 1 \in A \otimes H.$$

Using the isomorphism of Lemma 3.1, this means

$$\sum_{i=0}^{n} ((r_i)_{(0)} \otimes (r_i)_{(1)})(x \otimes 1)^i = \sum_{i=0}^{n} (r_i \otimes 1)(x \otimes 1)^i \in (R \otimes H)[x \otimes 1; \sigma \otimes \mathrm{id}_H, \delta \otimes \mathrm{id}_H].$$

By (O2) we must have $\rho_R(r_i) = r_i \otimes 1$ for all $0 \le i \le n$, so each r_i lies in R^{coH} and hence $p(x)$ is an element of $R^{coH}[x;\sigma,\delta]$. Then $A^{coH} = R^{coH}[x;\sigma,\delta]$. □

COROLLARY 3.3. *Let H be a K-Hopf algebra. Suppose that R is a right H-comodule algebra with structure map $\rho_R : R \to R \otimes H$, and let $A = R[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$ be an iterated skew polynomial ring over R such that each σ_i and δ_i are H-comodule morphisms, for $1 \le i \le n$. Then A is also a right H-comodule algebra with induced structure map $\rho_A : A \to A \otimes H$ given by*

$$\rho_A\left(\sum_{i=0}^{n} r_i X_i\right) = \sum_{i=0}^{n} (r_i)_{(0)} X_i \otimes (r_i)_{(1)}, \qquad \text{with } r_i \in R \text{ and } X_i \in \mathrm{Mon}(A),\, 0 \le i \le n.$$

Moreover, $A^{coH} = R^{coH}[x_1;\sigma_1,\delta_1]\cdots[x_n;\sigma_n,\delta_n]$, where σ_i and δ_i are considered restricted to $R^{coH}[x_1;\sigma_1,\delta_1]\cdots[x_{i-1};\sigma_{i-1},\delta_{i-1}]$, for every $1 \le i \le n$.

Now, we prove that for a certain type of skew polynomial rings, the Hopf Galois extension condition preserves.

THEOREM 3.4. *Let H be a $\Bbbk$-Hopf algebra, R a $\Bbbk$-algebra and $A = R[x;\sigma]$ a polynomial ring of endomorphism type over R such that R is a right H-comodule algebra and σ is an injective comodule morphism. If R is a right H-Galois object, then $\Bbbk[x;\sigma] \subset A$ is a right H-Galois extension.*

Proof. R being a right H-Galois object means that the map $\beta_R : R \otimes R \to R \otimes H$ given by

$$\beta_R(r \otimes s) = (r \otimes 1)\rho_R(s) = r s_{(0)} \otimes s_{(1)}, \qquad \text{for all } r, s \in R,$$

is bijective. For A, with the comodule structure induced by Proposition 3.2, we have that the

Galois map $\beta_A : A \otimes_{A^{coH}} A \to A \otimes H$ is given by

$$\beta_A\left(\sum_{i=0}^{n} r_i x^i \otimes \sum_{j=0}^{m} s_j x^j\right) = \left(\sum_{i=0}^{n} r_i x^i \otimes 1\right) \rho_A\left(\sum_{j=0}^{m} s_j x^j\right) = \left(\sum_{i=0}^{n} r_i x^i\right)\left(\sum_{j=0}^{m} (s_j)_{(0)} x^j\right) \otimes (s_j)_{(1)}. \quad (3.1)$$

β_A is injective: It is sufficient to show that, if for $r, s \in R$ and $i, j \in \mathbb{N}$ we have $\beta_A(r x^i \otimes s x^j) = 0$, then $r x^i \otimes s x^j = 0$. By (3.1) we have

$$0 = \beta_A(r x^i \otimes s x^j) = (r x^i)(s_{(0)} x^j) \otimes s_{(1)} \overset{(2.2)}{=} r\sigma^i(s_{(0)}) x^{i+j} \otimes s_{(1)}.$$

By the isomorphism of the Lemma 3.1, we have $(r\sigma^i(s_{(0)}) \otimes s_{(1)})(x+1)^{i+j} = 0$, which by (O2) means that

$$r\sigma^i(s_{(0)}) \otimes s_{(1)} = \beta_R(r \otimes \sigma^i(s)) = 0 \in R \otimes R.$$

By our hypothesis, it follows that $r \otimes \sigma^i(s) = 0$. Since the tensor product is taken over the field $\Bbbk$, by [Rom08, Theorem 14.5], it follows that $r = 0$ or $\sigma^i(s) = 0$. Hence, by the injectivity of σ, $r = 0$ or $s = 0$. Either case, $r x^i \otimes s x^j = 0$.

β_A is surjective: Recall the notation of Section 1.4,

$$\beta_R^{-1}(1 \otimes h) = h^{[1]} \otimes h^{[2]} \in R \otimes R, \qquad \text{for all } h \in H.$$

Then, for any $\sum_{i=0}^{n} r_i x^i \otimes h \in A \otimes H$, we have

$$\begin{aligned}
\beta_A\left(\sum_{i=0}^{n} r_i \sigma^i(h^{[1]}) x^i \otimes h^{[2]}\right) &= \beta_A\left(\sum_{i=0}^{n} r_i x^i h^{[1]} \otimes h^{[2]}\right) = \sum_{i=0}^{n} r_i x^i h^{[1]} h^{[2]}{}_{(0)} \otimes h^{[2]}{}_{(1)} \\
&= \left(\sum_{i=0}^{n} r_i x^i \otimes 1\right)(h^{[1]} h^{[2]}{}_{(0)} \otimes h^{[2]}{}_{(1)}) \overset{(1.49)}{=} \left(\sum_{i=0}^{n} r_i x^i \otimes 1\right)(1 \otimes h) \\
&= \sum_{i=0}^{n} r_i x^i \otimes h.
\end{aligned}$$

Thus β is bijective, as wanted. □

3.2 Almost symmetric algebras and Hopf Galois systems

We saw in Section 2.4 that for any almost symmetric algebra A, there exists a Lie algebra $\mathfrak{g}$ such that $\Bbbk \subset A$ is an $U(\mathfrak{g})$-extension. In this section, we shall give an alternative proof of that result using the equivalence between Hopf Galois objects, Hopf Galois systems and quantum torsors. For that, we must fist generalize Theorem 1.52.

Recall that any quantum K-torsor T has an associated map $\mu : T \to T \otimes T^{op} \otimes T$, which is denoted by $\mu(x) = x^{(1)} \otimes x^{(2)} \otimes x^{(3)}$, and a Grunspan map $\theta : T \to T$ satisfying

$$\theta(x) = x^{(1)} x^{(2)(3)} x^{(2)(2)} x^{(2)(1)} x^{(3)}.$$

We also recall the construction of the Hopf algebra $H_l(T)$ (resp. $H_r(T)$) defined in (1.58) (resp. (1.59)) as certain subalgebras of $T \otimes T^{op}$ (resp. $T^{op} \otimes T$). Summarizing Theorem 1.44, we have

that the elements of $H_l(T)$ are of the form $x_i \otimes y_i \in T \otimes T^{op}$ satisfying

$$x_i^{(1)} \otimes x_i^{(2)} \otimes \theta(x_i^{(3)}) \otimes y_i = x_i \otimes y_i^{(3)} \otimes y_i^{(2)} \otimes y_i^{(1)}.$$

Moreover, the comultiplication, counit and antipode on $H_l(T)$ are given by

$$\begin{aligned}\Delta_{H_l(T)}(x_i \otimes y_i) &= x_i^{(1)} \otimes x_i^{(2)} \otimes x_i^{(3)} \otimes y_i,\\ u_T\varepsilon_{H_l(T)}(x_i \otimes y_i) &= x_i y_i,\\ S_{H_l(T)}(x_i \otimes y_i) &= y_i \otimes \theta(x_i).\end{aligned}$$

Similarly, the elements of $H_r(T)$ are of the form $x_i \otimes y_i \in T^{op} \otimes T$ satisfying

$$x_i \otimes \theta(y_i^{(1)}) \otimes y_i^{(2)} \otimes y_i^{(3)} = x_i^{(3)} \otimes x_i^{(2)} \otimes x_i^{(1)} \otimes y_i,$$

and the comultiplication, counit and antipode are given by

$$\begin{aligned}\Delta_{H_r(T)}(x_i \otimes y_i) &= x_i \otimes y_i^{(1)} \otimes y_i^{(2)} \otimes y_i^{(3)},\\ u_T\varepsilon_{H_r(T)}(x_i \otimes y_i) &= x_i y_i,\\ S_{H_r(T)}(x_i \otimes y_i) &= \theta(y_i) \otimes x_i.\end{aligned}$$

In order to generalize Theorem 1.52 to the case when T is a faithfully flat $H_r(T)$-Galois object, we introduce a symmetric version of Hopf Galois systems.

DEFINITION 3.1 (TOTAL HOPF GALOIS SYSTEM, [GRU03, DEFINITION 3.1]). A *total K-Hopf Galois system* consists of two K-Hopf algebras A and B, and two K-algebras T and Z, satisfying the following axioms:

(THGS1) T is an A-B-bicomodule algebra with respective structure maps $\alpha_T : T \to A \otimes T$ and $\beta_T : T \to T \otimes B$.

(THGS2) Z is an B-A-bicomodule algebra with respective structure maps $\alpha_Z : Z \to Z \otimes A$ and $\beta_Z : Z \to B \otimes Z$.

(THGS3) There exist algebra morphisms $\gamma : A \to T \otimes Z$ and $\delta : B \to Z \otimes T$ such that:

$$\begin{aligned}(\gamma \otimes \mathrm{id}_T)\alpha_T &= (\mathrm{id}_T \otimes \delta)\beta_T,\\ (\mathrm{id}_Z \otimes \gamma)\alpha_z &= (\delta \otimes \mathrm{id}_Z)\beta_Z,\\ (\mathrm{id}_T \otimes \beta_Z)\gamma &= (\beta_T \otimes \mathrm{id}_Z)\gamma,\\ (\alpha_Z \otimes \mathrm{id}_T)\delta &= (\mathrm{id}_Z \otimes \alpha_T)\delta,\\ (\mathrm{id}_A \otimes \gamma)\Delta_A &= (\alpha_T \otimes \mathrm{id}_Z)\gamma,\\ (\gamma \otimes \mathrm{id}_A)\Delta_A &= (\mathrm{id}_T \otimes \alpha_Z)\gamma,\\ (\delta \otimes \mathrm{id}_B)\Delta_B &= (\mathrm{id}_Z \otimes \beta_T)\delta,\\ (\mathrm{id}_B \otimes \delta)\Delta_B &= (\beta_Z \otimes \mathrm{id}_T)\delta.\end{aligned}$$

(THGS4) There exist algebra morphisms $S_T : T \to Z^{op}$ and $S_Z : Z \to T^{op}$ such that:

$$\begin{aligned}
\gamma S_A &= \tau_{(12)}(S_T \otimes S_Z)\gamma, \\
\delta S_B &= \tau_{(12)}(S_z \otimes S_T)\delta, \\
\alpha_Z S_T &= \tau_{(12)}(S_A \otimes S_T)\alpha_T, \\
\beta_Z S_T &= \tau_{(12)}(S_T \otimes S_B)\beta_T, \\
\alpha_T S_Z &= \tau_{(12)}(S_Z \otimes S_A)\alpha_Z, \\
\beta_T S_Z &= \tau_{(12)}(S_B \otimes S_Z)\beta_Z, \\
m_T(\mathrm{id}_T \otimes S_Z)\gamma &= u_T\varepsilon_A, \\
m_T(S_Z \otimes \mathrm{id}_T)\delta &= u_T\varepsilon_B, \\
m_Z(S_T \otimes \mathrm{id}_Z)\gamma &= u_Z\varepsilon_A, \\
m_Z(\mathrm{id}_Z \otimes S_T)\delta &= u_Z\varepsilon_B.
\end{aligned}$$

Clearly, every Hopf Galois system (cf. Definition 1.42) is a total Hopf Galois system. Examples of total Hopf Galois systems can be found in [Gru03, §3].

THEOREM 3.5 ([GRU04, THEOREM 2]). *Let T be a faithfully flat quantum K-torsor with associated map μ and Grunspan map θ. Set $A = H_l(T)$, $B = H_r(T)$ and $\alpha_T : T \to A \otimes T$ and $\beta_T : T \to T \otimes B$ given by*

$$\begin{aligned}
\alpha_T(x) &= x^{(1)} \otimes x^{(2)} \otimes x^{(3)} \in A \otimes T \subset T \otimes T^{op} \otimes T, \\
\beta_T(x) &= x^{(1)} \otimes x^{(2)} \otimes x^{(3)} \in T \otimes B \subset T \otimes T^{op} \otimes T,
\end{aligned}$$

for all $x \in T$, which define a structure of A-B-biGalois object on T. Then the following assertions hold:

(i) $(B \otimes T)^{coB} = (T \otimes A)^{coH}$ *as subsets of* $T \otimes T \otimes T$.

(ii) *There is a natural structure of K-algebra on* $Z := (B \otimes T)^{coB} = (T \otimes A)^{coH}$ *as subalgebra of* $T^{op} \otimes T \otimes T^{op}$.

(iii) *There is a natural structure of B-A-biGalois object on Z given by the morphisms $\alpha_Z = Z \otimes \Delta_A : Z \to Z \otimes A$ and $\beta_Z = \Delta_B \otimes \mathrm{id}_T : Z \to B \otimes Z$.*

(iv) *If $x \in T$, then $S_T(x) = [(\theta \otimes \mathrm{id}_T \otimes \theta)\mu^{op}](x) \in Z$.*

(v) *The map $S_T : T \to Z^{op}$ is an algebra morphism.*

(vi) *If $x \in Z$, then $(\varepsilon_B \otimes \mathrm{id}_T)(x) = (\mathrm{id}_T \otimes \varepsilon_A)(x)$. We denote by $S_Z(x)$ this common value.*

(vii) *The map $S_Z : T \to T^{op}$ is an algebra morphism.*

(viii) *If $h = x_i \otimes y_i \in B \subset T^{op} \otimes T$, then*

$$\delta(h) = x_i \otimes y_i^{(1)} \otimes y_i^{(2)} \otimes y_i^{(3)} 1Z \otimes T \subset T^{op} \otimes T \otimes T^{op} \otimes T.$$

(ix) *If* $h = x_i \otimes y_i \in A \subset T \otimes T^{op}$, *then*

$$\gamma(h) = x_i^{(1)} \otimes x_i^{(2)} \otimes x_i^{(3)} \otimes y_i \in T \otimes Z \subset T \otimes T^{op} \otimes T \otimes Top.$$

(x) *The map* $\delta : B \to Z \otimes T$ *is an algebra morphism.*

(xi) *The map* $\gamma : A \to T \otimes Z$ *is an algebra morphism.*

Moreover, the quadruple (A, B, T, Z) *equipped with the morphism* $\alpha_T, \beta_T, \alpha_Z, \beta_Z, \gamma, \delta, S_T, S_Z$ *is a total Hopf-Galois system and the quantum torsor associated to this Hopf Galois system by Theorem 1.53 is isomorphic to* T. *In particular,* (A, B, T, Z) *and* (B, A, Z, T) *are two Hopf Galois systems.*

Given the full equivalence of (1.69), we immediately have the following result.

COROLLARY 3.6 ([GRU04, COROLLARY 1]). *Let* B *be a* K*-Hopf algebra and* T *a faithfully flat* B*-Galois object. Then there exists a Hopf algebra* A*, an algebra* Z *and algebra morphisms* $S_T : T \to Z^{op}$ *and* $S_Z : Z \to T^{op}$ *such that* (A, B, T, Z) *is a total Hopf Galois system. In particular,* (A, B, T, Z) *and* (B, A, Z, T) *are two Hopf Galois systems.*

Using Theorem 2.16 and Corollary 3.6, we have that almost symmetric algebras are examples of Hopf Galois systems.

THEOREM 3.7 ([GRU04, THEOREM 3]). *Let* $\mathfrak{g}$ *be a* $\Bbbk$*-Lie algebra and* $f \in Z^2(\mathfrak{g}, \Bbbk)$. *Consider the Sridharan enveloping algebras* $U_f(\mathfrak{g})$ *and* $U_{-f}(\mathfrak{g})$, *and define* $\gamma : U(\mathfrak{g}) \to U_f(\mathfrak{g}) \otimes U_{-f}(\mathfrak{g})$ *and* $\delta : U(\mathfrak{g}) \to U_{-f}(\mathfrak{g}) \otimes U_f(\mathfrak{g})$ *as*

$$x \mapsto 1 \otimes x + x \otimes 1, \qquad \text{for all } x \in \mathfrak{g},$$

and $S : U_{-f}(\mathfrak{g}) \to U_f(\mathfrak{g})$ *as*

$$S(x) = -x, \qquad \text{for all } x \in \mathfrak{g}.$$

Then, $(U(\mathfrak{g}), U(\mathfrak{g}), U_f(\mathfrak{g}), U_{-f}(\mathfrak{g}))$ *is a* $\Bbbk$*-Hopf Galois system.*

By the equivalence theorems of Section 1.5, we have the following immediate results.

COROLLARY 3.8 ([GRU04, COROLLARIES 2 AND 3]). *Let* $\mathfrak{g}$ *be a* $\mathbb{Q}$*-Lie algebra and* $f \in Z^2(\mathfrak{g}, \mathbb{Q})$. *Then the following assertions for the Sridharan algebra* $U_f(\mathfrak{g})$ *hold:*

(i) $U_f(\mathfrak{g})$ *is a quantum* $\Bbbk$*-torsor with associated map* $\mu(x) = x \otimes 1 - 1 \otimes x \otimes 1 + 1 \otimes 1 \otimes x$, *for* $x \in \mathfrak{g}$, *and Grunspan map* $\theta = \mathrm{id}_{U_f(\mathfrak{g})}$. *Moreover,* $H_l(U_f(\mathfrak{g})) \cong H_r(U_f(\mathfrak{g})) \cong U(\mathfrak{g})$.

(ii) $U_f(\mathfrak{g})$ *is a* $U(\mathfrak{g})$*-*$U(\mathfrak{g})$*-biGalois object.*

3.3 KASHIWARA ALGEBRAS AND QUANTUM TORSORS

In [Kas91] were defined a type of algebras which are useful in the study of crystal bases. In this section we introduce the preliminaries for such algebras and then prove that they are examples of Hopf Galois systems. Throughout, we assume that $\Bbbk = \mathbb{Q}$.

DEFINITION 3.2 (GENERALIZED CARTAN MATRIX, [KAC90, §1.1]). A square matrix $A = [a_{ij}]_{i,j=1}^{n}$ with entries in $\mathbb{Z}$ is called a *generalized Cartan matrix*, if it satisfies the following conditions:

$$\begin{aligned} a_{ii} &= 2 \qquad \text{for } 1 \le i \le n, \\ a_{ij} &\le 0 \qquad \text{for } i \ne j, \\ a_{ij} &= 0 \qquad \text{if and only if} \qquad a_{ji} = 0. \end{aligned}$$

The matrix A is said to be *indecomposable*, if for every pair of nonempty subsets $I_1, I_2 \subseteq I = \{1, \dots, n\}$ with $I_1 \cup I_2 = I$, there exists some $i \in I_1$ and $j \in I_2$ such that $a_{ij} \ne 0$.

REMARK 21. Throughout we will suppose that every generalized Cartan matrix is *symmetrizable*, i.e., there exists a diagonal matrix D with entries in $\mathbb{Z}_{>0}$ such that DA is symmetric.

Let $P^\vee$ be a free abelian group of rank $2n - \operatorname{rank}(A)$ with a $\mathbb{Z}$-basis

$$\{h_i : 1 \le i \le n\} \cup \{d_s : s = 1, \dots, n - \operatorname{rank}(A)\}.$$

$P^\vee$ is known as the *dual weight lattice*. The $\Bbbk$-linear space spanned by $P^\vee$, $\mathfrak{h} := \Bbbk \otimes_{\mathbb{Z}} P^\vee$, is called *the Cartan subalgebra*. We also define the *weight lattice* to be $P := \{\lambda \in \mathfrak{h}^* : \lambda(P^\vee) \subset \mathbb{Z}\}$.

The elements of a linear independent subset $\Pi := \{\alpha_i : 1 \le i \le n\} \subset \mathfrak{h}^*$ satisfying

$$\alpha_j(h_i) = a_{ij} \qquad \text{and} \qquad \alpha_j(d_s) \in \{0, 1\}, \qquad \text{for all } 1 \le i, j \le n \text{ and } s = 1, \dots, n - \operatorname{rank}(A),$$

are called *simple roots*. Similarly, each element of the set $\Pi^\vee := \{h_i : 1 \le i \le n\}$ is called a *simple coroots*.

DEFINITION 3.3 (CARTAN DATUM, [HK02, DEFINITION 2.1.1]). Let $A = [a_{ij}]_{i,j=1}^{n}$ be a generalized Cartan matrix. The quintuple $(A, \Pi, \Pi^\vee, P, P^\vee)$ defined as above is said to form a *Cartan datum* associated to A.

Recall that if V is a $\Bbbk$-vector space, the set $\mathfrak{gl}(V)$ of all $\Bbbk$-linear maps on V acquires a Lie algebra structure via the Lie bracket $[x, y] = xy - yx$, for all $x, y \in \mathfrak{gl}(V)$, and it is called the *general linear Lie algebra*. If $V = \Bbbk^n$, we denote the general linear Lie algebra by $\mathfrak{gl}(n, \Bbbk)$. Now, given a Lie algebra $\mathfrak{g}$ we define a Lie morphism $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$, called *the adjoint representation of* $\mathfrak{g}$, given by

$$\operatorname{ad} x(y) = [x, y], \qquad \text{for all } x, y \in \mathfrak{g}.$$

Whit this, we are able to define a type of algebras of great relevance; they are consider as a generalization of semisimple Lie algebra to the infinite dimensional case (cf. [Kac90, Chapter 1]).

DEFINITION 3.4 (KAC-MOODY ALGEBRA, [HK02, DEFINITION 2.1.3]). Let $(A, \Pi, \Pi^\vee, P, P^\vee)$ be a Cartan datum associated to a generalized Cartan matrix $A = [a_{ij}]_{i,j=1}^{n}$. The *Kac-Moody algebra* associated to the Cartan datum is the $\Bbbk$-Lie algebra generated by the elements e_i, f_i $(1 \le i \le n)$ and $h \in P^\vee$ subject to the following defining relations:

(KMA1) $[h, h'] = 0$ for all $h, h' \in P^\vee$,

(KMA2) $[e_i, f_j] = \delta_{ij} h_i$ for all $i, j \in I$,

(KMA3) $[h, e_i] = \alpha_i(h) e_i$ for all $i \in I$ and $h \in P^\vee$,

(KMA4) $[h, f_i] = -\alpha_i(h) f_i$ for all $i \in I$ and $h \in P^\vee$,

(KMA5) $(\operatorname{ad} e_i)^{1-a_{ij}} e_j = 0$ for all $i \neq j$, $i, j \in I$,

(KMA6) $(\operatorname{ad} f_i)^{1-a_{ij}} f_j = 0$for all $i \neq j$, $i, j \in I$.

(KMA1)-(KMA4) are called the *Weyl relations*, while (KMA5)-(KMA6) are known as the *Serre relations*.

Given a Kac-Moody algebra $\mathfrak{g}$ associated to the Cartan datum $(A, \Pi, \Pi^\vee, P, P^\vee)$, we define an inner product on $\mathfrak{h}^*$ such that

$$(\alpha_i, \alpha_i) \in \mathbb{N} \qquad \text{and} \qquad \langle h_i, \lambda \rangle = 2(\alpha_i, \lambda)/(\alpha_i, \alpha_i), \qquad \text{for all } \lambda \in \mathfrak{h}^*.$$

Our base ring is $K := \mathbb{Q}[[\hbar]]$, the formal power series ring over $\mathbb{Q}$. We also set $q = \exp(\hbar)$, $q_i = q^{\langle \alpha_i, \alpha_i \rangle/2}$, $t_i = q^{h_i}$,

$$[n]_i = \frac{q_i^n - q_i^{-n}}{q_i - q_i^{-1}} \qquad \text{and} \qquad [n]_i! = \prod_{k=1}^{n} [k]_i.$$

Definition 3.5 (Kashiwara algebra). The *Kashiwara algebra* $B_q(\mathfrak{g})$ is the associative K-algebra generated by the elements e_i', f_i $(1 \leq i \leq n)$ and $q^h, h \in \bigoplus_{i=1}^n \mathbb{Z} h_i$ $(h_i \in \Pi^\vee)$ together with the relations:

$$\begin{gathered}
q^h e_i' q^{-h} = q^{\langle h, \alpha_i \rangle} e_i', \\
q^h f_i q^{-h} = q^{-\langle h, \alpha_i \rangle} f_i, \\
e_i' f_j = q_i^{\langle h_i, \alpha_j \rangle} f_j e_i' + \delta_{ij}, \\
\sum_{k=0}^{1-\langle h_i, \alpha_k \rangle} (-1)^k X_i^{(k)} X_j X_i^{(1-\langle h_i, \alpha_j \rangle)} = 0,
\end{gathered}$$

where $X = e', f$ and $X_i^{(n)} = X_i^n / [n]_i!$.

Theorem 3.9 ([Gru04, Theorem 4]). *Let $B := B_q(\mathfrak{g})$ be a Kashiwara algebra. Then the map $\mu : B \to B \otimes B^{op} \otimes B$ defined by*

$$\begin{aligned}
\mu(e_i') &:= 1 \otimes 1 \otimes e_i' - 1 \otimes e_i' t_i \otimes t_i^{-1} + e_i' \otimes t_i \otimes t_i^{-1}, \\
\mu(f_i) &= 1 \otimes 1 \otimes f_i - 1 \otimes f_i t_i \otimes t_i^{-1} + f_i \otimes t_i \otimes t_i^{-1}, \\
\mu(q^h) &= q^h \otimes q^{-h} \otimes q^h,
\end{aligned}$$

makes B into a quantum torsor. Moreover, the Grunspan map $\theta : B \to B$ is given by

$$\theta(e_i') = t_i^{-1} e_i' t_i, \qquad \theta(f_i) t_i^{-1} f_i t_i \qquad \text{and} \qquad \theta(q^h) = q^h.$$

Using characterization theorems, [Gru04, §4.2] gives an explicit description of the two algebras $H_l(B)$ and $H_r(B)$ that can be attached to the torsor, endowing it with a Hopf Galois system.

APPENDIX A

GRADED AND FILTERED RINGS

Since the *filtration-graduation technique* was used in this work, for the purpose of a self-contained document, in this Appendix we review the basic notions regarding filtered and graded rings/algebras. Definitions and results are adapted from [MR01], [Lez19c] and [Lod98].

DEFINITION A.1 (GRADED RING). A ring A is said to be $\mathbb{Z}$-*graded* if there exist a family $\{A_p\}_{p\in\mathbb{Z}}$ of its additive group A^+ satisfying the following conditions:

(G1) $A_pA_q \subseteq A_{p+q}$, for all $p, q \in \mathbb{Z}$,

(G2) $A = \bigoplus_{p\in\mathbb{Z}} A_p$, as an abelian group.

Furthermore, if A is a $\Bbbk$-algebra, we addition the following condition:

(G3) A_p is a $\Bbbk$-subspace, for every $p \in \mathbb{Z}$.

The family $\{A_p\}_{p\in\mathbb{Z}}$ is called a *grading* of A, the subgroup A_p (for any $p \in \mathbb{Z}$) is called the *homogeneous component of degree p* and any non-zero element of A_p is said to be *homogeneous of degree p*. Moreover, if $A_p = 0$ for $p < 0$, we say that A is $\mathbb{N}$-*graded*.

Homogeneous elements of degree p will be usually denoted with the subscript p, emphasizing its degree.

As we saw in Example 1.20, graduations can be taken over any group G and not necessarily over $\mathbb{Z}$. However, for our purposes, is enough to consider this particular case. Also notice that every ring (resp. $\Bbbk$-algebra) A has a *trivial graduation* given by

$$A_0 := A \qquad \text{and} \qquad A_p := 0, \qquad \text{for all } p \in \mathbb{Z} - \{0\}.$$

Throughout this Appendix, all graduations considered will be non-trivial.

REMARK. By (G1), A_0 is a subring (resp. subalgebra) of A. Furthermore, $1 \in A_0$. Indeed, by (G2) we can write $1 = a_0 + a_{p_1} + \cdots + a_{p_t}$; if $x = b_{q_1} + \cdots + b_{q_l}$ is an arbitrary element of A expanded in homogeneous components, then for $1 \leq i \leq l$,

$$b_{q_i} = 1b_{q_i} = a_0b_{q_i} + a_{p_1}b_{q_i} + \cdots + a_{p_t}b_{q_i}.$$

Since the sum in (G2) is direct, comparing degrees we must have $a_0 b_{q_i} = b_{q_i}$ for all $1 \leq i \leq l$. Hence $a_0 x = x$. Similarly, we get $x a_0 = x$ and therefore $a_0 = 1 \in A_0$ ($a_{p_1} = \cdots = a_{p_t} = 0$).

DEFINITION A.2 (GRADED MORPHISM). Let $A = \bigoplus_{p\in\mathbb{Z}} A_p, B = \bigoplus_{p\in\mathbb{Z}} B_p$ be two $\mathbb{Z}$-graded rings (resp. $\Bbbk$-algebras). A ring (resp. $\Bbbk$-algebra) morphism $f : A \to B$, is said to be *graded* if $f(A_p) \subseteq B_p$, for every $p \in \mathbb{Z}$.

DEFINITION A.3 (CONNECTED ALGEBRA). Let $A = \bigoplus_{p\in\mathbb{N}} A_p$ be a $\mathbb{N}$-graded $\Bbbk$-algebra. A is said to be *connected*, if $A_0 = \Bbbk$.

Since (G2) demands the sum to be direct, not necessarily every two-sided ideal of a graded ring A will preserve the graduation for A/I. Hence we have the following result characterizing the ideals preserving the graduation.

PROPOSITION A.1. *Let $A = \bigoplus_{p\in\mathbb{Z}} A_p$ be a $\mathbb{Z}$-graded ring (resp. $\Bbbk$-algebra) and I an ideal of A. Then the following assertions are equivalent:*

(i) $I = \bigoplus_{p\in\mathbb{Z}} (A_p \cap I)$.

(ii) *If $a \in I$, then every homogeneous component of a is also an element of I.*

(iii) *I is generated (as ideal) by homogeneous elements.*

(iv) *The quotient A/I is $\mathbb{Z}$-graded, with $(A/I)_p = (A_p + I)/I$ for every $p \in \mathbb{Z}$.*

If I is a two-sided ideal of A which satisfies one of the previous assertions, we say that I is *graded* or *homogeneous*.

We now define filtered rings.

DEFINITION A.4 (FILTERED RING). A ring A is said to be $\mathbb{Z}$-*filtered* if there exist a family $\{F_p(A)\}_{p\in\mathbb{Z}}$ of its additive group A^+ satisfying the following conditions:

(F1) $F_p(A)F_q(A) \subseteq F_{p+q}(A)$, for all $p, q \in \mathbb{Z}$,

(F2) For $p < q$, $F_p(A) \subseteq F_q(A)$,

(F3) $A = \bigcup_{p\in\mathbb{Z}} F_p(A)$,

(F4) $1 \in F_0(A)$.

Furthermore, if A is a $\Bbbk$-algebra, we addition the following condition:

(F5) $F_p(A)$ is a $\Bbbk$-subspace, for every $p \in \mathbb{Z}$.

The family $\{F_p(A)\}_{p\in\mathbb{Z}}$ is called a *filtration* of A. The filtration is said to be *separated* if additionally $\bigcap_{p\in\mathbb{Z}} F_p(A) = 0$. Moreover, if $F_{-1}(A) = 0$, we say that A is $\mathbb{N}$-*filtered*.

REMARK. From conditions (F1) and (F4) is immediate that $F_0(A)$ is a subring (resp. subalgebra) of A. Also notice that every $\mathbb{N}$-filtration is separated.

DEFINITION A.5 (FILTERED MORPHISM). Let A, B be two rings (resp. $\Bbbk$-algebras) with respective filtrations $\{F_p(A)\}_{p\in\mathbb{Z}}$ and $\{F_p(A)\}_{p\in\mathbb{Z}}$. A ring (resp. $\Bbbk$-algebra) morphism $f : A \to B$ is said to be *filtered*, if $f(F_p(A)) \subseteq F_p(A)$, for every $p \in \mathbb{Z}$.

A filtered morphism $f : A \to B$ is called *strict* if $f(F_p(A)) = \mathrm{Im}(f) \cap F_p(B)$, for every $p \in Z$.

As in the graded case, one can ask when a quotient A/I of a filtered ring (algebra) A is also filtered; while for that case, conditions over the ideal I have to be imposed, for filtrations all ideals work.

PROPOSITION A.2. *Let A be a filtered ring (resp. $\Bbbk$-algebra) with filtration $\{F_p(A)\}_{p\in\mathbb{Z}}$. If I is an ideal of A then A/I has a $\mathbb{Z}$-filtration given by*

$$F_p(A/I) := (F_p(A) + I)/I, \qquad \text{for all } p \in \mathbb{Z}.$$

Notice that every $\mathbb{Z}$-graded ring (resp. $\Bbbk$-algebra) $A = \bigoplus_{p\in\mathbb{Z}} A_p$ has an induced filtration, given by

$$F_p(A) = \bigoplus_{n\leq p} A_n, \qquad \text{for all } p \in \mathbb{Z}. \tag{A.1}$$

Reciprocally, we have the following result.

PROPOSITION A.3. *Let A be a $\mathbb{Z}$-filtered ring (resp. $\Bbbk$-algebra) with filtration $\{F_p(A)\}_{p\in\mathbb{Z}}$. Then there exists a $\mathbb{Z}$-graded ring (resp. $\Bbbk$-algebra) associated to A, denoted by* $\mathrm{gr}(A)$.

Proof. We define, for every $p \in \mathbb{Z}$, the abelian group

$$\mathrm{gr}(A)_p := F_p(A)/F_{p-1}(A)$$

and set $\mathrm{gr}(A) := \bigoplus_{p\in\mathbb{Z}} \mathrm{gr}(A)_p$. $\mathrm{gr}(A)$ is obviously and abelian group. Moreover, the rule

$$(a + F_{p-1}(A))(b + F_{q-1}(A)) := ab + F_{p+q-1}(A), \qquad \text{for all } a, b \in A,$$

induces a multiplication in $\mathrm{gr}(A)$. The verification of (G1) and (G2) is straightforward from the construction. Furthermore, if A is a $\Bbbk$-algebra, every $\mathrm{gr}(A)_p$ is a quotient of $\Bbbk$-spaces and therefore a $\Bbbk$-space itself. □

COROLLARY A.4. *Let $A = \bigoplus_{p\in\mathbb{Z}} A_p$ be a $\mathbb{Z}$-graded ring (resp. $\Bbbk$-algebra). Then* $\mathrm{gr}(A) \cong A$.

Proof. We know that $\{F_p\}_{p\in\mathbb{Z}}$ is a $\mathbb{Z}$-filtration for A, where F_p is defined as in (A.1). Hence

$$\mathrm{gr}(A)_p = \frac{\left(\bigoplus_{n\leq p} A_n\right)}{\left(\bigoplus_{n\leq p-1} A_n\right)} \cong A_p, \qquad \text{for all } p \in \mathbb{Z},$$

and thus we have $\mathrm{gr}(A) = \bigoplus_{p\in\mathbb{Z}} \mathrm{gr}(A)_p \cong \bigoplus_{p\in\mathbb{Z}} A_p \cong A$ as abelian groups (resp. $\Bbbk$-vector spaces). It is clear that the isomorphism also respects multiplications. □

The next result shows that, in categorical terms, $\mathrm{gr}(-)$ can be seen as a functor between the category of $\mathbb{Z}$-filtered rings (resp. $\Bbbk$-algebras) and the category of $\mathbb{Z}$-graded rings (resp. $\Bbbk$-algebras).

PROPOSITION A.5. *Let A, B be two $\mathbb{Z}$-filtered rings (resp. $\Bbbk$-algebras) with respective filtrations $\{F_p(A)\}_{p\in\mathbb{Z}}$, $\{F_p(B)\}_{p\in\mathbb{Z}}$. If $f : A \to B$ is a filtered morphism, then there exists a graded morphism $\mathrm{gr}(f) : \mathrm{gr}(A) \to \mathrm{gr}(B)$. Moreover, if f is strict and injective (resp. surjective, bijective), then $\mathrm{gr}(f)$ is also injective (resp. surjective, bijective).*

Proof. Since f is a filtered morphism, we have $f(F_p(A)) \subseteq F_p(B)$, for every $p \in \mathbb{Z}$. Hence for any $p \in \mathbb{Z}$ we can induce the function $\mathrm{gr}(f)_p : \mathrm{gr}(A)_p = F_p(A)/F_{p-1}(A) \to \mathrm{gr}(B) = F_p(B)/F_{p-1}(B)$ given by

$$\mathrm{gr}(f)_p(a_p + F_{p-1}(A)) := f(a_p) + F_{p-1}(B), \qquad \text{for all } a_p \in F_p(A).$$

Notice that $\mathrm{gr}(f)_p$ is a group (resp. $\Bbbk$-linear) morphism. Therefore we can consider the map $\mathrm{gr}(f) := \bigoplus_{p\in\mathbb{Z}} \mathrm{gr}(f)_p$ given by

$$\mathrm{gr}(f)((a_p + F_{p-1}(A))_{p\in\mathbb{Z}}) = (f(a_p) + F_{p-1}(B))_{p\in\mathbb{Z}} \qquad \text{for all } (a_p + F_{p-1}(A))_{p\in\mathbb{Z}} \in \mathrm{gr}(A).$$

One can easily check that $\mathrm{gr}(f)$ is, in fact, a ring (resp. $\Bbbk$-algebra) morphism which, by construction, is graded.

Suppose that f is injective and strict. If $(a_p + F_{p-1}(A))_{p\in\mathbb{Z}} \in \mathrm{gr}(A)$ is such that

$$\mathrm{gr}(f)((a_p + F_{p-1}(A))_{p\in\mathbb{Z}} \in \mathrm{gr}(A)) = 0,$$

then by construction we have $f(a_p) + F_{p-1}(B) = 0$ for every $p \in \mathbb{Z}$, meaning that $f(a_p) \in F_{p-1}(B) \cap \mathrm{Im}(f) = f(F_{p-1}(A))$. Hence, for every $p \in \mathbb{Z}$, there exists $a'_{p-1} \in F(A)_{p-1}$ such that $f(a_p) = f(a'_{p-1})$. Since f is injective, we have $a_p = a'_{p-1}$ and thus $a_p + F_{p-1}(A) = F_{p-1}(A)$, for every $p \in \mathbb{Z}$. Then $\mathrm{gr}(f)$ is injective.

Now, suppose that f is surjective and strict. Given $(b_p + F_{p-1}(B))_{p\in\mathbb{Z}} \in \mathrm{gr}(B)$, we have that for every b_p there exists $a \in A$ such that $f(a) = b_p$ and hence $b_p \in F_p(B) \cap \mathrm{Im}(f) = f(F_p(A))$. Then there exists $a_p \in F_p(A)$ such that $f(a_p) = b_p$. It is obvious that $\mathrm{gr}(f)((a_p + F_{p-1}(A))_{p\in\mathbb{Z}}) = (f(a_p) + F_{p-1}(B))_{p\in\mathbb{Z}}$, implying that $\mathrm{gr}(f)$ is surjective. □

PROPOSITION A.6. *Let A, B be two $\mathbb{N}$-filtered rings (resp. $\Bbbk$-algebras) with respective filtration $\{F_p(A)\}_{p\in\mathbb{N}}$, $\{F_p(B)\}_{p\in\mathbb{N}}$. If $f : A \to B$ is a filtered morphism such that $\mathrm{gr}(f) : \mathrm{gr}(A) \to \mathrm{gr}(B)$ is injective (resp. surjective, bijective), then f is also injective (resp. surjective, bijective).*

Proof. For every $p \in \mathbb{N}$, we denote by $F_p(f) : F_p(A) \to F_p(B)$ the restriction of f to $F_p(A)$. Notice that $F_p(f)$ is a group morphism, for every $p \in \mathbb{N}$. Moreover, $F_0(f)$ is injective (resp. surjective, bijective). Indeed, since $\mathrm{gr}(f)$ is injective (resp. surjective, bijective), then every $\mathrm{gr}(f)_p$ is also injective (resp. surjective, bijective); in particular, $\mathrm{gr}(f)_0 : \mathrm{gr}(A)_0 = F_0(A) \to \mathrm{gr}(B) = F_0(B)$ which by construction coincides with $F_0(f)$.

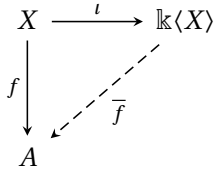
We assume by induction that $F_{p-1}(f)$ is injective (resp. surjective, bijective). Hence we can consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & F_{p-1}(A) & \hookrightarrow & F_p(A) & \twoheadrightarrow & \mathrm{gr}(A)_p & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle F_{p-1}(f)} & & \downarrow{\scriptstyle F_p(f)} & & \downarrow{\scriptstyle \mathrm{gr}(f)_p} & & \\
0 & \longrightarrow & F_{p-1}(B) & \hookrightarrow & F_p(B) & \twoheadrightarrow & \mathrm{gr}(B)_p & \longrightarrow & 0
\end{array}$$

Since $F_{p-1}(f)$ and $\mathrm{gr}(f)_p$ are injective (resp. surjective, bijective) and each row is exact, By the Short Five Lemma (cf. [Hun74, Lemma IV.1.17]), the map $f_p(f)$ is also injective (resp. surjective, bijective). Since $p \in \mathbb{N}$ was arbitrary, by (F3), the assertion of the proposition is clear. □

Several properties of $\mathrm{gr}(A)$ can be transfered to A, such as being an integral domain (cf. [MR01, 1.6.6(i)]), prime ring (cf. [MR01, 1.6.6(ii)]) or left (right) Noetherian (cf. [MR01, 1.6.9]). Since the associated graded ring has usually a nicer behavior than the original one, the study of $\mathrm{gr}(A)$ is a powerful tool in non-commutative algebra. We review some examples treated in this document.

EXAMPLE A.1 (FREE ALGEBRA). Let X be a non-empty set. A $\Bbbk$-algebra $\Bbbk\langle X\rangle$ is said to be a *free algebra over X* if there exists a function $\iota : X \to \Bbbk\langle X\rangle$ such that the following universal property is satisfied: f*or any $\Bbbk$-algebra A and any function $f : X \to A$ there exists an unique algebra morphism $\overline{f} : \Bbbk\langle X\rangle \to A$ such that the following diagram is commutative:*



It can be shown that $\Bbbk\langle X\rangle$ is unique up to isomorphism (cf. [Coh03, Section 6.2]) and that any element of this algebra is a finite $\Bbbk$-linear combination of *words*, each being of the form $x_1 \cdots x_p$ with $x_1, \ldots, x_p \in X$; the *empty word* is accepted and denoted by e. We say that the *degree* of a word $w := x_1 \cdots x_p$ is p and we denote $\mathrm{gr}(w) = p$; moreover, $\mathrm{gr}(e) := 0$. The degree of an arbitrary element f of $\Bbbk\langle X\rangle$ is defined as the maximum degree of the words that comprise it; f is said to be *homogeneous* if all of its words have the same grade.

For every $p \in \mathbb{N}$ we define

$$\Bbbk\langle X\rangle_p := \{f \in \Bbbk\langle X\rangle : f \text{ is homogeneus of degree } p\} \cup \{0\}.$$

Notice that $\{\Bbbk\langle X\rangle_p\}_{p\in\mathbb{N}}$ is a $\mathbb{N}$-graduation for $\Bbbk\langle X\rangle$. Moreover, with this graduation, $\Bbbk\langle X\rangle$ is connected.

EXAMPLE A.2 (POLYNOMIAL RING). Let R be a ring and $R[x_1, \ldots, x_n]$ the classical multivariate polynomial ring over R (cf. Example 2.1). Recall that an element $f \in R[x_1, \ldots, x_n]$ is said to be *homogeneous* if if all of its monomials have the same grade. The canonical $\mathbb{N}$-graduation of $R[x_1, \ldots, x_n]$ is given by

$$R[x_1, \ldots, x_n]_p := \{f \in R[x_1, \ldots, x_n] : f \text{ is homogeneus of degree } p\} \cup \{0\}, \qquad \text{for every } p \in \mathbb{N}.$$

Indeed, for $X = \{x_1, \ldots, x_n\}$, we have $R[x_1, \ldots, x_n] \cong \Bbbk\langle X\rangle / I$, where I is the homogeneous ideal generated by $x_i x_j = x_j x_i$, for all $1 \leq i, j \leq n$.

EXAMPLE A.3 (TENSOR ALGEBRA). Let V a $\Bbbk$-vector space and $T(V)$ its tensor algebra (cf. Example 1.6). A $\mathbb{N}$-graduation for $T(V)$ is given by $T(V)_p := V^{\otimes p}$, for every $p \in \mathbb{N}$. Notice that with this graduation, $T(V)$ is connected.

EXAMPLE A.4 (SYMMETRIC ALGEBRA). Let V a $\Bbbk$-vector space and $S(V)$ its symmetric algebra

(cf. Example 1.7). Since the ideal I defined in (1.10) is homogeneous, by Proposition A.1, the quotient $S(V) = T(V)/I$ is also $\mathbb{N}$-graded. Moreover, since I is proper,

$$S(V)_0 = (T(V)/I)_0 = (T(V)_0 + I)/I = (\Bbbk + I)/I = \Bbbk,$$

making $S(V)$ into a connected algebra.

CONCLUSIONS AND FUTURE WORK

The implicit aim of this work was to create a picture of the current state of Hopf Galois theory and, in parallel, the interactions with remarkable classes of non-commutative rings, together with numerous examples.

We have presented useful and basic preliminaries of Hopf algebras in Chapter 1. However, beyond our scope there are many topics that can be reviewed in the literature. Perhaps, our merit is to develop and expand tedious calculations that usually are omitted in the literature. The same can be said for Hopf Galois extensions themselves.

As mentioned and shown throughout the document, non-commutative polynomial algebras appear in a wide range of applications and contexts. Nevertheless, the families presented in Chapter 2 are not the only ones in the literature (e.g. G-algebras [Lev05] or PI rings [MR01]) and hence their interactions with coactions of Hopf algebras and Hopf Galois extensions themselves are still unknown.

On the other hand, Hopf Galois theory has for itself several open problems and fronts of investigation. Although we mention some of them at the end of Section 1.3, we recall a few: (co)homology calculations, generalization to tensor and Hom-Hopf categories, theory for Hopf grupoids, Morita equivalences in more general contexts, etc. And, related with Sections 1.4 and 1.5, also several questions appear, such as classification problems, more characterization theorems or generalizations.

Finally, we ask below some specific questions that came up during the realization of this work.

QUESTION 1. Is there a generalization of Lemma 3.1 for (skew) PBW extensions? That question was partially answered in [RS17c, Proposition 3.1]. An interesting case of future study for us is the enveloping algebra of an arbitrary algebra A, which is defined as $A^e := A \otimes A^{op}$.

QUESTION 2. Is there an analogue of Proposition 1.2 for (skew) PBW extensions? We have found some problems in the calculations but soon we hope to have a full answer.

QUESTION 3. Are the conditions of Theorem 3.4 only sufficient but not necessary? Can we generalize it to skew polynomial rings in general? What about (skew) PBW extensions?

QUESTION 4. Is there a generalization of Hopf Galois systems such that they turn out to be equivalent to Hopf Galois extensions (not just Hopf Galois objects)?

QUESTION 5. Are we able to find more examples of quantum torsor and Hopf Galois systems? Are

they also members of our families of non-commutative rings? Can we find a non-commutative geometric sense to them?

QUESTION 6. The dual of a quantum torsor is known as a quantum cotorsor. Is there any relation between them and the notion of Hopf Galois coextension presented in [Has12]?

QUESTION 7. Can we extend the notion of quantum torsor and Hopf Galois systems to the context of Hopf grupoids?

BIBLIOGRAPHY

[Aco14] J. P. Acosta. Ideales primos en extensiones PBW torcidas. Master's thesis, Universidad Nacional de Colombia Sede Bogotá, 2014. 86, 89

[AK08] E. Aljadeff and C. Kassel. Polynomial Identities and Noncommutative Versal Torsors. *Adv. Math.*, 218(5):1453–1495, 2008. 52

[AL15] J. Acosta and O. Lezama. Universal Property of Skew PBW Extensions. *Algebra Discrete Math.*, 20(1):1–12, 2015. 86, 90

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969. 3

[AS02] N. Andruskiewitsch and H.-J. Schneider. Pointed Hopf Algebras. In S. Montgomery and H.-J. Schneider, editors, *New Directions in Hopf Algebras*, volume 43 of *Mathematical Sciences Research Institute Publications*, pages 1–68. Cambridge University Press, 2002. 52

[AW10] K. Ardakov and S. Wadsley. On the Cartan Map for Crossed Products and Hopf-Galois Extensions. *Algebr. Represent. Theory*, 13(1):33–41, 2010. 51

[Bö05] G. Böhm. Galois Theory for Hopf Algebroids. *Ann. Univ. Ferrara Sez. VII Sci. Mat.*, 51(1):233–262, 2005. 51

[Bae09] J. Baez. Torsors Made Easy, 2009. http://math.ucr.edu/home/baez/torsors.html. 41, 53

[BCV16] E. Batista, S. Caenepeel, and J. Vercruysse. Hopf Categories. *Algebr. Represent. Theory*, 19(5):1173–1216, 2016. 52

[Bel00] A. D. Bell. Comodule Algebras and Galois Extensions Relative to Polynomial Algebras, Free Algebras, and Enveloping Algebras. *Comm. Algebra*, 28(1):337–362, 2000. 94

[Ber78] G. M. Bergman. The Diamond Lemma for Ring Theory. *Adv. Math.*, 29(2):178–218, 1978. 86

[Ber92] R. Berger. The Quantum Poincaré-Birkhoff-Witt Theorem. *Commun Math Phys*, 143(2):215–234, 1992. 88

[BF12] T. Brzeziński and S. A. Fairfax. Bundles over Quantum Real Weighted Projective Spaces. *Axioms*, 1(2):201–225, 2012. 39, 40, 41, 42

[BG88] A. D. Bell and K. R. Goodearl. Uniform Rank Over Differential Operator Rings and Poincaré-Birkhoff-Witt Extensions. *Pacific J. Math.*, 131(1):13–37, 1988. IV, 82

[BH04] T. Brzeziński and P. Hajac. The Chern-Galois Character. *C.R. Math.*, 338(2):113–116, 2004. 42, 51

[BH09] T. Brzezinski and P. Hajac. Galois-Type Extensions and Equivariant Projectivity. *arXiv preprint arXiv:0901.0141*, 2009. 42

[BHMS06] P. F Baum, P. Hajac, R. Matthes, and W. Szymanski. Noncommutative Geometry Approach to Principal and Associated Bundles. *arXiv preprint math/0701033*, 2006. 39, 40

[Bic01] J. Bichon. Cosovereign Hopf algebras. *J. Pure Appl. Algebra*, 157(2-3):121–133, 2001. 71

[Bic03a] J. Bichon. Hopf-Galois Systems. *J. Algebra*, 264(2):565–581, 2003. III, 66, 67, 68, 69, 70, 71

[Bic03b] J. Bichon. The Representation Category of the Quantum Group of a Non-Degenerate Bilinear Form. *Comm. Algebra*, 31(10):4831–4851, 2003. 70

[BOZZ15] K. A. Brown, S. O'Hagan, J. J. Zhang, and G. Zhuang. Connected Hopf Algebras and Iterated Ore Extensions. *J. Pure Appl. Algebra*, 219(6):2405–2433, 2015. IV

[Cal16] F. Calderón. Construcción de álgebras de Hopf mediante extensiones de Ore, 2016. Bachelor's thesis. III

[CCMT07] S. Caenepeel, S. Crivei, A. Marcus, and M. Takeuchi. Morita Equivalences Induced by Bimodules Over Hopf-Galois Extensions. *J. Algebra*, 314(1):267–302, 2007. 52

[CF18] S. Caenepeel and T. Fieremans. Descent and Galois Theory for Hopf Categories. *J. Algebra Appl.*, 17(07):1850120, 2018. 52

[CFM90] M. Cohen, D. Fischman, and S. Montgomery. Hopf Galois Extensions, Smash Products, and Morita Equivalence. *J. Algebra*, 133(2):351–372, 1990. 47, 49, 50

[CHR65] S. U. Chase, D. K. Harrison, and A. Rosenberg. *Galois Theory and Cohomology of Commutative Rings*, volume 52 of *Memories of the American Mathematical Society*. American Mathematical Society, 1965. III

[CM10] S. Caenepeel and A. Marcus. Hopf-Galois Extensions and an Exact Sequence for H-Picard Groups. *J. Algebra*, 323(3):622–657, 2010. 52

[Coh85] P. M. Cohn. *Free Rings and Their Relations*. London Mathematical society Monographs. Academic Press, second edition, 1985. III

[Coh98] R. L. Cohen. *The Topology of Fiber Bundles: Lecture Notes*. Stanford Univeristy, 1998. http://math.stanford.edu/~ralph/fiber.pdf. 40

[Coh03] P. M. Cohn. *Basic Algebra: Groups, Rings and Fields*. Springer London, first edition, 2003. 110

[CQR07] F. Chyzak, A. Quadrat, and D. Robertz. OreModules: A Symbolic Package for the Study of Multidimensional Linear Systems. In J. Chiasson and J. J. Loiseau, editors, *Applications of Time Delay Systems*, volume 352 of *Lecture Notes in Control and Information Sciences*. Springer, 2007. 81, 82

[CS69] S. U. Chase and M. E. Sweedler. *Hopf Algebras and Galois Theory*, volume 97 of *Lecture Notes in Mathematics*. Springer Verlag, 1969. III, 26, 27, 28

[CWW03] S. Caenepeel, D. Wang, and Y. Wang. Twistings, Crossed Coproducts, and Hopf-Galois Coextensions. *Internat. J. Math. Math. Sci.*, 2003(69):4325–4345, 2003. 51

[CZ16] Y. Chen and L. Zhang. Hopf-Galois Extensions for Monoidal Hom-Hopf Algebras. *Colloq. Math.*, 143:1–21, 2016. 43

[DGH01] L. Dąbrowski, H. Grosse, and P. Hajac. Strong Connections and Chern-Connes Pairing in the Hopf-Galois Theory. *Commun. Math. Phys.*, 220(2):301–331, 2001. 42

[DMR96] S. Dăscălescu, G. Militaru, and Ş. Raianu. Crossed Coproducts and Cleft Coextensions. *Comm. Algebra*, 24(4):1229–1243, 1996. 51

[DNR01] S. Dăscălescu, C. Năstăsescu, and Ş. Raianu. *Hopf Algebras: An Introduction*, volume 235 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., first edition, 2001. 2, 3, 5, 6, 7, 8, 10, 12, 13, 16, 17, 19, 20, 21, 24, 28, 29, 35, 46

[Doi90] Y. Doi. Hopf Extensions of Algebras and Maschke Type Theorems. *Israel J. Math.*, 72(1–2):99, 1990. 50, 70

[Doi93] Y. Doi. Braided Bialgebras and Quadratic Blalgebras. *Comm. Algebra*, 21(5):1731–1749, 1993. 69, 70

[Dom17] Z. Domotor. Torsor Theory of Physical Quantities and their Measurement. *Meas. Sci. Rev.*, 17(4):152–177, 2017. 41

[DT86] Y. Doi and M. Takeuchi. Cleft Comodule Algebras for a Bialgebra. *Comm. Algebra*, 14(5):801–817, 1986. 48

[DT89] Y. Doi and M. Takeuchi. Hopf-Galois Extensions of Algebras, the Miyashita-Ulbrich Action, and Azumaya Algebras. *J. Algebra*, 121(2):488–516, 1989. 43

[Dur94] M. Durđević. Geometry of Quantum Principal Bundles II - Extended Version. *arXiv preprint q-alg/9412005*, 1994. 43

[Dur95] M. Durđević. Quantum Principal Bundles as Hopf-Galois Extensions. *arXiv preprint q-alg/9507022*, 1995. 43

[DVL90] M. Dubois-Violette and G. Launer. The Quantum Group of a Non-Degenerate Bilinear Form. *Phys. Lett. B*, 245(2):175–177, 1990. 70

[DW96] A. V. Daele and S. Wang. Universal Quantum Groups. *Internat. J. Math.*, 07(02):255–263, 1996. 71

[Fri00] T. Friedrich. *Dirac Operators in Riemannian Geometry*, volume 25 of *Graduate Studies in Mathematics*. American Mathematical Society, 2000. 40

[GK91] A. M. Gavrilik and A. U. Klimyk. q-Deformed Orthogonal and Pseudo-Orthogonal Algebras and Their Representations. *Lett. Math. Phys.*, 21(3):215–220, 1991. 89

[GL11] C. Gallego and O. Lezama. Gröbner Bases for Ideals of σ-PBW Extensions. *Comm. Algebra*, 39(1):50–75, 2011. IV, 85, 86, 87, 90

[GP87] C. Greither and B. Pareigis. Hopf Galois Theory for Separable Field Extensions. *J. Algebra*, 106(1):239–258, 1987. 30

[Gru03] C. Grunspan. Quantum Torsors. *J. Pure Appl. Algebra*, 184(2-3):229–255, 2003. III, 53, 57, 61, 63, 64, 69, 100, 101

[Gru04] C. Grunspan. Hopf-Galois Systems and Kashiwara Algebras. *Comm. Algebra*, 32(9):3373–3389, 2004. 101, 102, 104, 105

[Gün99] R. Günther. Crossed Products for Pointed Hopf Algebras. *Comm. Algebra*, 27(9):4389–4410, 1999. 43

[GW04] K. R. Goodearl and R. B. Jr Warfield. *An Introduction to Noncommutative Noetherian Rings*, volume 61 of *London Mathematical Society Student Texts*. Cambridge University Press, 2004. 73, 74, 75, 76, 77, 78

[Hal03] B. C. Hall. *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*, volume 222 of *Graduate Texts in Mathematics*. Springer, 2003. 13

[Has12] M. Hassanzadeh. Hopf Galois Coextensions in Noncommutative Geometry. *arXiv preprint arXiv:1204.1883*, 2012. 51, 113

[Hay90] T. Hayashi. q-Analogues of Clifford and Weyl Algebras-Spinor and Oscillator Representations of Quantum Enveloping Algebras. *Commun Math Phys*, 127(1):129–144, 1990. 90

[Hel01] S. Helgason. *Differential Geometry and Symmetric Spaces*, volume 341. American Mathematical Society, 2001. 13

[Hes09] K. Hess. Homotopic Hopf Galois Extensions: Foundations and Examples. In A. Baker and B. Richter, editors, *New topological contexts for Galois theory and algebraic geometry (BIRS 2008)*, volume 16 of *Geometry and Topology Monographs*, pages 79–132. Mathematical Sciences Publishers, 2009. 52

[HK02] J. Hong and S.-J. Kang. *Introduction to Quantum Groups and Crystal Bases*, volume 42 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002. 103

[HKP00] M. Havlíček, A. U. Klimyk, and S. Pošta. Central Elements of the Algebras $u'_q(\mathrm{so}_\mathrm{m})$ and $u_q(\mathrm{iso}_\mathrm{m})$. *Czechoslovak J. Phys.*, 50(1):79–84, 2000. 89

[HR13] M. Hassanzadeh and B. Rangipour. Equivariant Hopf Galois Extensions and Hopf Cyclic Cohomology. *J. Noncommut. Geom.*, 7(1):105–133, 2013. 51

[Hum72] J. E. Humphreys. *Introduction to Lie Algebras and Representation Theory*, volume 9 of *Graduate Texts in Mathemathics*. Springer Verlag, 1972. 13

[Hun74] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1974. 10, 11, 29, 110

[Hus94] D. Husemöller. *Fibre Bundles*, volume 20 of *Graduate texts in mathematics*. Springer New York, third edition, 1994. 39

[HZ17] J. He and Y. Zhang. Cohen-Macaulay Invariant Subalgebras of Hopf Dense Galois Extensions. *arXiv preprint arXiv:1711.04197*, 2017. 52

[Jac79] N. Jacobson. *Lie Algebras*. Dover Books on Advanced Mathematics. Dover Publications, Inc., first edition, 1979. 13

[Jac85] N. Jacobson. *Basic Algebra I*. W. H. Freeman and Company, second edition, 1985. 29, 30

[Jat84] V. A. Jategaonkar. A Multiplicative Analog of the Weyl Algebra. *Comm. Algebra*, 12(14):1669–1688, 1984. 88

[JBSZ81] A. Jannussis, G. Bbodimas, D. Soublas, and V. Zisis. Remarks on the q-Quantization. *Lett. Nuovo Cimento*, 30(4):123–127, 1981. 88

[JR18] J. Jaramillo and A. Reyes. Symmetry and Reversibility Properties for Quantum Algebras and Skew Poincaré-Birkhoff-Witt Extensions. *Ingeniería y Ciencia*, 14(27):29–52, 2018. 90

[JŞ06] P. Jara and D. Ştefan. Hopf-Cyclic Homology and Relative Cyclic Homology of Hopf-Galois Extensions. *Proc. London Math. Soc. (3)*, 93(1):138–174, 2006. 51, 93

[Kac90] V. G. Kac. *Infinite-Dimensional Lie Algebras*. Cambridge University Press, 1990. 103

[Kas91] M. Kashiwara. On crystal bases of the q-analogue of universal enveloping algebras. *Duke Math. J.*, 63(2):465–516, 1991. 102

[Kas95] C. Kassel. *Quantum Groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, first edition, 1995. 8, 9, 13, 14

[Kas09] C. Kassel. Generic Hopf Galois Extensions. In M. Marcolli and D. Parashar, editors, *Proceedings of the Workshop on Quantum Groups and Noncommutative Geometry*, Max-Planck Series, pages 104–120. Vieweg Verlag, 2009. 52

[Kay19] N. Z. Kayvan. Skew Braces and Hopf-Galois Structures of Heisenberg Type. *J. Algebra*, 524:187–225, 2019. 44

[Kha15] V. Kharchenko. *Quantum Lie Theory: A Multilinear Approach*, volume 2150 of *Letures Notes in Mathematics*. Springer, 2015. 15

[KJJ15] M. Kauers, M. Jaroschek, and F. Johansson. Ore Polynomials in Sage. In *Lecture Notes in Computer Science*, volume 8942, pages 105–125. Springer International Publishing, 2015. 79

[KS05] C. Kassel and H.-J. Schneider. Homotopy Theory of Hopf Galois Extensions. *Ann. Inst. Fourier (Grenoble)*, 55(7):2521–2550, 2005. 52

[KT81] H. Kreimer and M. Takeuchi. Hopf Algebras and Galois Extensions of an Algebra. *Indiana Univ. Math. J.*, 30(5):675–692, 1981. III, 26, 27, 48

[Kur80] M. V. Kuryshkin. Opérateurs quantiques généralisés de création et d'annihilation. *Ann. Fond. Louis de Broglie*, 5:111–125, 1980. 87

[Kur02] V. L. Kurakin. Hopf Algebra Dual to a Polynomial Algebra over a Commutative Ring. *Math. Notes*, 71(5/6):617–623, 2002. 10

[Lev05] V. Levandovskyy. *Non-Commutative Computer Algebra for Polynomial Algebras: Gröbner Bases, Applications and Implementation*. PhD thesis, Universität Kaiserslautern, 2005. 86, 112

[Lez19a] O. Lezama. *Cuadernos de Álgebra, No. 3: Módulos*. SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, Colombia, 2019. https://sites.google.com/a/unal.edu.co/sac2/. 75

[Lez19b] O. Lezama. *Cuadernos de Álgebra, No. 4: Álgebra lineal*. SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, Colombia, 2019. https://sites.google.com/a/unal.edu.co/sac2/. 11

[Lez19c] O. Lezama. *Cuadernos de Álgebra, No. 9: Álgebra no conmutativa*. SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, Colombia, 2019. https://sites.google.com/a/unal.edu.co/sac2/. 13, 73, 74, 77, 78, 79, 83, 106

[Li02] H. Li. *Noncommutative Gröbner Bases and Filtered-Graded Transfer*, volume 1795 of *Lecture Notes in Mathematics*. Springer Berlin Heidelberg, 2002. 87

[LL17] E. Latorre and O. Lezama. Non-Commutative Algebraic Geometry of Semi-Graded Rings. *Internat. J. Algebra Comput.*, 27(04):361–389, 2017. 90

[Lod98] J.-L. Loday. *Cyclic Homology*, volume 301 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 1998. 91, 106

[Man18] Y. I. Manin. *Quantum Groups and Noncommutative Geometry*. CRM Short Courses. Springer International Publishing, second edition, 2018. 88

[Mas94] A. Masoka. Cleft Extensions for a Hopf Algebra Generated by a Nearly Primitive Element. *Comm. Algebra*, 22(11):4537–4559, 1994. 43

[Mon93] S. Montgomery. *Hopf Algebras and Their Actions on Rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. American Mathematical Society, 1993. 1, 2, 4, 6, 7, 8, 10, 15, 16, 18, 19, 20, 21, 24, 26, 28, 29, 31, 34, 37, 38, 43, 45, 46, 48, 49

[Mon09] S. Montgomery. Hopf Galois Theory: A Survey. In A. Baker and B. Richter, editors, *New topological contexts for Galois theory and algebraic geometry (BIRS 2008)*, volume 16 of *Geometry and Topology Monographs*, pages 367–400. Mathematical Sciences Publishers, 2009. 19, 22, 24, 28, 32, 33, 34, 35, 38, 43, 45, 48, 49, 50

[MR01] J. C. McConnell and J. C. Robson. *Noncommutative Noetherian Rings*, volume 30 of *Graduate Studies in Mathematics*. American Mathematical Society, 2001. 12, 48, 49, 72, 73, 74, 79, 85, 106, 110, 112

[MS99] S. Montgomery and H.-J. Schneider. Prime Ideals In Hopf Galois Extensions. *Israel J. Math.*, 112(1):187–235, 1999. 51

[MS09] D. Marciniak and M. Szamotulski. Galois Theory of Hopf Galois Extensions. *arXiv preprint arXiv:0912.0291*, 2009. 50

[MŞ10] A. Makhlouf and D. Ştefan. Coactions on Hochschild Homology of Hopf-Galois Extensions and Their Coinvariants. *J. Pure Appl. Algebra*, 214(9):1654–1677, 2010. 51

[Nus91] P. Nuss. L'homologie cyclique des algèbres enveloppantes des algèbres de lie de dimension trois. *J. Pure Appl. Algebra*, 73(1):39–71, 1991. 94

[NvO04] C. Năstăsescu and F. van Oystaeyen. *Methods of Graded Rings*. Springer Berlin Heidelberg, 2004. 31

[Ols16] M. Olsson. *Algebraic Spaces and Stacks*. American Mathematical Society, 2016. 41

[Ore33] Ø. Ore. Theory of Non-Commutative Polynomials. *Ann. of Math. (2)*, 34(3):480–508, 1933. III, 72

[Pan03] A. Panov. Ore Extensions of Hopf Algebras. *Math. Notes*, 74(3):401–410, 2003. IV

[Par90] B. Pareigis. Forms of Hopf Algebras and Galois Theory. *Banach Center Publ.*, 26(1):75–93, 1990. 30

[Rad76] D. E. Radford. The Order of the Antipode of a Finite Dimensional Hopf Algebra is Finite. *Amer. J. Math.*, 98(2):333–355, 1976. 49

[Rap18] Á. Raposo. The Algebraic Structure of Quantity Calculus. *Meas. Sci. Rev.*, 18(4):147–157, 2018. 41

[Rey13] A. Reyes. *Ring and Module Theoretic Properties of σ-PBW Extensions*. PhD thesis, Universidad Nacional de Colombia Sede Bogotá, 2013. 86

[Rog08] J. Rognes. *Galois Extensions of Structured Ring Spectra/Stably Dualizable Groups*, volume 192 of *Memories of the American Mathematical Society*. American Mathematical Society, 2008. 44

[Rom06] S. Roman. *Field Theory*, volume 158 of *Graduate Texts in Mathematics*. Springer-Verlag New York, second edition, 2006. 62

[Rom08] S. Roman. *Advanced Linear Algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer New York, third edition, 2008. 99

[Ros95] A. Rosenberg. *Noncommutative Algebraic Geometry and Representations of Quantized Algebras*, volume 330 of *Mathematics and its Applications*. Springer Netherlands, 1995. 89

[RS17a] A. Reyes and H. Suárez. A Notion of Compatibility for Armendariz and Baer Properties Over Skew PBW Extensions. *Rev. Un. Mat. Argent.*, pages 157–178, 2017. 90

[RS17b] A. Reyes and H. Suárez. Bases for Quantum Algebras and Skew Poincaré-Birkhoff-Witt Extensions. *Momento*, 1(54):54–75, 2017. 90

[RS17c] A. Reyes and H. Suárez. Enveloping Algebra and Skew Calabi-Yau Algebras Over Skew Poincaré-Birkhoff-Witt Extensions. *Far East J. Math. Sci.*, 102(2):373–397, 2017. 90, 112

[RS17d] A. Reyes and H. Suárez. PBW Bases for Some 3-Dimensional Skew Polynomial Algebras. *Far East J. Math. Sci.*, 101(6):1207–1228, 2017. 90

[RS18a] A. Reyes and H. Suárez. Skew Poincaré-Birkhoff-Witt Extensions Over Weak Zip Rings. *Beitr. Algebra. Geom.*, 2018. 90

[RS18b] A. Reyes and Y. Suárez. On the ACCP in Skew Poincaré-Birkhoff-Witt Extensions. *Beitr. Algebra. Geom.*, 59(4):625–643, 2018. 90

[Rum98] D. Rumynin. Hopf–Galois Extensions with Central Invariants and Their Geometric Properties. *Algebr. Represent. Theory*, 1(4):353–381, 1998. 51

[Sch90a] H.-J. Schneider. Principal Homogeneous Spaces for Arbitrary Hopf Algebras. *Israel J. Math.*, 72(1-2):167–195, 1990. 50

[Sch90b] H.-J. Schneider. Representation Theory of Hopf Galois Extensions. *Israel J. Math.*, 72(1-2):196–231, 1990. 23, 44, 50, 57

[Sch92] P. Schauenburg. *Tannaka Duality for Arbitrary Hopf Algebras*, volume 66 of *Algebra Berichte*. Reinhard Fischer Verlag, 1992. 68

[Sch96] P. Schauenburg. Hopf Bigalois Extensions. *Comm. Algebra*, 24(12):3797–3825, 1996. 28, 50, 64, 69, 70

[Sch97] P. Schauenburg. A Bialgebra That Admits a Hopf-Galois Extension Is a Hopf Algebra. *Proc. Amer. Math. Soc.*, 125(1):83–85, 1997. 29

[Sch98] P. Schauenburg. Galois Correspondences for Hopf Bigalois Extensions. *J. Algebra*, 201(1):53–70, 1998. 50

[Sch99] P. Schauenburg. Galois Objects over Generalized Drinfeld Doubles, with an Application to $u_q(\mathrm{sl}_2)$. *J. Algebra*, 217(2):584–598, 1999. 43

[Sch02] P. Schauenburg. Quantum Torsors and Hopf-Galois Objects. *arXiv preprint math/0208047*, 2002. 58, 59, 64

[Sch03] P. Schauenburg. Quantum Torsors with Fewer Axioms. *arXiv preprint math/0302003*, 2003. 53, 54, 55, 57, 61

[Sch04] P. Schauenburg. Hopf-Galois and Bi-Galois Extensions. In G. Janelidze, B. Pareigis, and W. Tholen, editors, *Galois Theory, Hopf Algebras, and Semiabelian Categories*, volume 43 of *Fields Institute Communications*, pages 469–515. American Mathematical Society, 2004. 28, 29, 65, 66

[Skr04] S. Skryabin. Hopf Galois Extensions, Triangular Structures, and Frobenius Lie Algebras in Prime Characteristic. *J. Algebra*, 277(1):96–128, jul 2004. 43

[Smi92] S. P. Smith. Quantum Groups: An Introduction and Survey for Ring Theorists. In *Noncommutative rings*, volume 24 of *Mathematical Sciences Research Institute Publications*, pages 131–178. Springer New York, 1992. 88

[Sri61] R. Sridharan. Filtered Algebras and Representations of Lie Algebras. *Trans. Amer. Math. Soc.*, 100(3):530–550, 1961. 91, 92, 93

[SS05] P. Schauenburg and H.-J. Schneider. On Generalized Hopf Galois Extensions. *J. Pure Appl. Algebra*, 202(1-3):168–194, 2005. 42, 51

[Şte95] D. Ştefan. Hochschild Cohomology on Hopf Galois Extensions. *J. Pure Appl. Algebra*, 103(2):221–233, 1995. 51

[Swe69] M. E. Sweedler. *Hopf Algebras*. Mathematical Lectures Note Series. W. A. Benjamin Inc., New York, 1969. 4, 8

[Taf71] E. J. Taft. The Order of the Antipode of Finite-Dimensional Hopf Algebra. *Proc. Natl. Acad. Sci.*, 68(11):2631–2633, 1971. 14

[Tak71] M. Takeuchi. Free Hopf Algebras Generated by Coalgebras. *J. Math. Soc. Japan*, 23(4):561–582, 1971. 71

[Tsa18] C. Tsang. Hopf-Galois Structures on a Galois S_n-Extension. *arXiv preprint arXiv:1812.06419*, 2018. 44

[vOZ94] F. van Oystaeyen and Y. Zhang. Galois-Type Correspondences for Hopf Galois Extensions. *K-Theory*, 8(3):257–269, 1994. 50

[vU81] K. H. von Ulbrich. Vollgraduierte Algebren. *Abh. Math. Semin. Univ. Hambg.*, 51(1):136–148, 1981. 31

[vU82] K. H. von Ulbrich. Galoiserweiterungen von nichtkommutativen Ringen. *Comm. Algebra*, 10(6):655–672, 1982. 48

[Wal85] R. Wallisser. Rationale Approximation des q-Analogues der Exponentialfunktion und Irrationalitätsaussagen für diese Funktion. *Arch. Math.*, 44:59–64, 1985. 89

[Yu16] X. Yu. Hopf-Galois Objects of Calabi-Yau Hopf Algebras. *J. Algebra Appl.*, 15(10):165–194, 2016. 43

[ZZ03] S. Zhang and Y.-Z. Zhang. Hopf Galois Extension in Braided Tensor Categories. *arXiv preprint math/0309448*, 2003. 52